Functional Requirements and Test Cases (FRTC)

VERSION 1.3.0

FIPS 201 EVALUATION PROGRAM

March 2, 2015

Office of Government wide Policy
Office of Technology Strategy
Identity Management Division
Washington, DC 20405

Document History

Status	Version	Date	Comment	Audience
Draft	0.0.1		Document creation.	Limited
Draft	0.0.2	4/30/2013	Added background and objectives text, normative references.	Limited
Draft	0.1.0	4/30/2013	Full comment resolution version for review.	Limited
Draft	0.1.1	5/1/2013	Release candidate 1.	Limited
Draft	0.1.2	5/2/2013	Revised per May 1, 2013 EPTWG Meeting.	Limited
Draft	0.1.3	5/6/13	Draft Release.	EPTWG
Draft	1.0.0 RC1	7/16/2013	Final review for program release.	Limited
Draft	1.0.1 RC2	7/19/2013	QA updates approved.	Limited
RC1	1.1.2	8/21/2013	Final release.	Public
RC2	1.1.3	8/29/2013	Minor fixes.	Limited
RC3	1.1.4	9/4/2013	CHUID deprecated; Credential # anti-collision specs added; Remove optional technologies.	Limited
RC4	1.1.5	9/12/2013	Requirements for allowing PKI processing to be degraded and logging of failed certificates.	Limited
RC5	1.1.6	9/20/2013	Improved credential processing; added 6 hour CRL requirement; added FICA< mode = no legacy; fixed path names; restored missing path tests 22-35; identified invalid test cases.	Limited
Final	1.2.0	10/23/2013	Updated per initial testing for public release; used Reverse BCD format for 128-bit FASC-N; labeled incorrect tests for future update; identified test cases that will no longer be tested.	Public
Draft	1.3.0	3/2/2015	• 3/14/14 – First edit for errata. • 4/16/14 – Second errata edit. Updated document publication schedule. Removed Test Number column. Added Appendix 2, Deprecated Functional Requirements and test Cases. Update for PIV in E-PACS v3.0. Test section numbers static. • 6/2/14 – Fixed cached Public Key test cases; re-worded [Sect508] requirement, added severity level info, re-wrote publication schedule with severities in mind. Added Appendix 3, Severity Levels, to describe the severity level concept. • 7/6/14 – Added Mobile Handheld Requirements. • 3/2/15 – Removed deprecated items from the PKI Paths Table and moved them to new Appendix 3, Deprecated ICAM PKI Paths (old Appendix 3 moved to Appendix 4). Deleted tables and other content no longer needed (e.g., date dependent items where the date is now in the past / no longer applicable).	Limited

Table of Contents

1 Background

The General Services Administration (GSA) is responsible for supporting the adoption of interoperable and standards-based Identity, Credential, and Access Management (ICAM) technologies throughout the Federal Government. As part of that responsibility, GSA operates and maintains the Federal Information Processing Standard (FIPS) 201 Evaluation Program and its FIPS 201 Approved Products List (APL), as well as services for Federal ICAM (FICAM) conformance and compliance.

2 Change Control

This document is a living document, and is expected to be updated over time as new or revised functional requirements are identified. In addition, this document will be updated in accordance with the following schedule:

1. A new version will be published no less than one year from issuance of the current version.
2. If security or infrastructure risks are identified, an interim release may occur.

All new versions are effective immediately. New or revised requirements and their test cases will include an effective date, commensurate with their assigned severity level (see *Appendix 1*and *Appendix 4*).

All approved Physical Access Control Systems (PACS) solutions must pass testing against new and revised requirements before their effective date or be moved to the Removed Products List (RPL).

Notification of changes will be sent to the Evaluation Program Technical Working Group (EPTWG) email list.

3 Objectives

This document identifies the functional requirements that the FIPS 201 Evaluation Program will perform on PACS submitted for evaluation. All requirements are instrumented using a smart card as presented to the system and various Public Key Infrastructure (PKI) paths. The PKI and smart cards test for specific common failures in cards and PKI, as well as Advanced Persistent Threat (APT) issues that impact PACS specifically. The PACS evaluation process is designed to be agnostic to architecture and focuses solely on functional testing using an end-to-end testing methodology.

4 Test Instrumentation

For PACS, the FIPS 201 Evaluation Program relies on fully-defined, instrumented testing. This requires two core elements:

1. ***ICAM Test Cards*** – There are two cards that are completely valid and well formed. In addition, there are cards that have injected faults assuming day-to-day operational errors, and cards emulating a well-funded attacker.
2. ***Test PKI*** – Provides the ability to link golden test cards with PKI faults, which provides the mechanism needed to verify that the system under test honors the PKI.

The full testing regimen, leveraging these test instruments, is described in *Appendix 1*.

4.1 ICAM Cards Used in Test

The following cards are used in the FIPS 201 Evaluation Program.

- Live PIV and PIV-I Cards from various issuers;
- ICAM Test Cards[1] (detailed in *Table 1*);
- NIST PIV Test Cards; and
- DoD JITC CAC Test Cards.

Table 1 - ICAM Test Cards Used in Test

ICAM Test Card	Description	Threat Type
1	Golden PIV	None
2	Golden PIV-I	None
3	Substituted keypair in PKI-AUTH certificate	Manipulated Data
4	Tampered CHUID	Manipulated Data
5	Tampered PIV and Card Authentication Certificates	Manipulated Data
6	Tampered PHOTO	Manipulated Data
7	Tampered FINGERPRINT	Manipulated Data
8	Tampered SECURITY OBJECT	Manipulated Data
9	Expired CHUID signer	Invalid Date
10	Expired certificate signer	Invalid Date
11	PIV Authentication Certificate expiring after CHUID	Invalid Date
12	Authentication certificates valid in future	Invalid Date
13	Expired authentication certificates	Invalid Date
14	Expired CHUID	Invalid Date
15	Valid CHUID copied from one card to another **(PIV)**	Copied Credential
16	Valid Card Authentication Certificate copied from one card to another **(PIV)**	Copied Credential
17	Valid PHOTO copied from one card to another **(PIV)**	Copied Credential

[1] All [FRTC] tests leveraging ICAM Cards 25-29 will be run when these cards become available.

ICAM Test Card	Description	Threat Type
18	Valid FINGERPRINT copied from one card to another **(PIV)**	Copied Credential
19	Valid CHUID copied from one card to another **(PIV-I)**	Copied Credential
20	Valid Card Authentication Certificate copied from one card to another **(PIV-I)**	Copied Credential
21	Valid PHOTO copied from one card to another **(PIV-I)**	Copied Credential
22	Valid FINGERPRINT copied from one card to another **(PIV-I)**	Copied Credential
23	Private and Public Key replaced	Manipulated Keys
24	Revoked authentication certificates	Revoked Credential
25	Discovery object is not present	Only Application PIN is present and shall be used.
26	Discovery object tag 0x5F2F is present First byte: 0x40, Second byte 0x00	Only Application PIN is present and shall be used.
27	Discovery object tag 0x5F2F is present First byte: 0x60, Second byte: 0x10	Application and Global PINs are present. Application PIN is primary.
28	Discovery object tag 0x5F2F is present First byte: 0x60, Second byte: 0x20	Application and Global PINs are present. Global PIN is primary.
29	Discovery object is present and tag 0x5F2F is not populated	Only Application PIN is present and shall be used.

4.2 PKI Used in Test

Table 2 describes the PKI infrastructure used for the FIPS 201 Evaluation Program. Deprecated path have been migrated to *Appendix 3*.

Table 2 - ICAM PKI Path Descriptions

ICAM PKI Path Number	Fault description	Operational Group
1	ICAM Invalid CA Signature	Manipulated Data
2	ICAM Invalid CA *notBefore* Date	Revoked/Date Invalid
3	ICAM Invalid CA *notAfter* Date	Revoked/Date Invalid
4	ICAM Invalid Name Chaining	Standards Conformant Processing
5	ICAM Missing Basic Constraints	Standards Conformant Processing
6	ICAM Invalid CA False Critical	Manipulated Data

ICAM PKI Path Number	Fault description	Operational Group
7	ICAM Invalid CA False not Critical	Standards Conformant Processing
8	ICAM Invalid Path Length Constraint	Standards Conformant Processing
9	ICAM *keyUsage keyCertSign* False	Standards Conformant Processing
10	ICAM keyUsage Not Critical	Standards Conformant Processing
11	ICAM *keyUsage* Critical *CRLSign* False	Standards Conformant Processing
12	ICAM Invalid *inhibitPolicyMapping*	Standards Conformant Processing
13	ICAM Invalid DN *nameConstraints*	Standards Conformant Processing
14	ICAM Invalid SAN *nameConstraints*	Standards Conformant Processing
15	ICAM Invalid Missing CRL	Standards Conformant Processing
16	ICAM Invalid Revoked CA	Revoked/Date Invalid
17	ICAM Invalid CRL Signature	Manipulated Data
18	ICAM Invalid CRL Issuer Name	Standards Conformant Processing
19	ICAM Invalid Old CRL *nextUpdate*	Revoked/Date Invalid
20	ICAM Invalid CRL *notBefore*	Revoked/Date Invalid
21	ICAM Invalid *distributionPoint*	Standards Conformant Processing
22	ICAM Valid *requiredExplicitPolicy*	Standards Conformant Processing
23	ICAM Invalid *requiredExplicitPolicy*	Standards Conformant Processing
24	ICAM Valid GeneralizedTime	PKI/Crypto Compatibility
25	ICAM Invalid GeneralizedTime	Standards Conformant Processing
32	ICAM Invalid SKID	Standards Conformant Processing
33	ICAM Invalid AKID	Standards Conformant Processing
34	ICAM Invalid CRL format	Standards Conformant Processing
35	ICAM 4096bit RSA key	PKI/Crypto Compatibility
36	ICAM Invalid CRL Signer	Standards Conformant Processing
37	ICAM OCSP Expired Responder Certificate	Invalid Date
38	ICAM OCSP Revoked OCSP Responder	Revoked Credential

ICAM PKI Path Number	Fault description	Operational Group
39	ICAM OCSP *nocheck* not present Revoked OCSP Responder	Standards Conformant Processing
40	ICAM OCSP Invalid Signature OCSP responder	Manipulated Data

5 Credential Number Processing

Table 3 describes the minimal set of credential number processing rules. All solutions shall use 128-bit (16 byte) credential numbers to provide full protection against credential number collisions. These credential numbers shall be processed and stored in binary format. It is strongly recommended that credential numbers not be parsed into separate fields for interoperability, audit, and ease of testing purposes (see Test Cases 7.5.1, 7.5.2, and 7.8.3). If the system parses the numbers into separate fields, it must be stored in such a way that the 128-bit credential can be viewed from the user interface or through reporting in its original 128bit format. The details of how the credential is parsed shall be provided to the GSA ICAM Lab for testing purposes. The FIPS 201 Evaluation Program anticipates new categories that have direct interaction with E-PACS (e.g., PSIM and PIAM). These new categories are anticipated to require that credential numbers be stored in a single field.

Table 3 – Minimal Set of Credential Number Processing Rules

FASC-N Rule	
PIV and CAC: 128 Bit Output (Reverse BCD) FASC-N ID + CS + ICI + Pers Inden + Org Cat + Org Ind + Pers/Org (parity automatically removed)	Serial Output: 13 41 00 01 98 76 54 11 12 34 56 78 90 11 34 11

	Decoded Wiegand Data:
	`1    3    4    1  - 0    0    0    1  - 9    8    7    6`
	`0001 0011 0100 0001-0000 0000 0000 0001-1001 1000 0111 0110`
	`5    4  - 1  - 1  - 1    2    3    4    5    6    7    8`
	`0101 0100-0001-0001-0001 0010 0011 0100 0101 0110 0111 1000`
	`9    0  - 1  - 1    3    4    1  - 1`
	`1001 0000-1000-1000 1100 0010 1000-1000`

	Translated Card Data: Agency Code = 1341, System Code = 0001, Credential Number = 987654, CS = 1, ICI = 1, PI = 1234567890, OC = 1, OI = 1341, POA = 1
UUID Rule	
PIV and PIV-I: 128 Bit UUID	16-byte binary representation of the UUID as defined by [RFC 4530].

6 Normative References

[BAA] Buy American Act Certification FAR 52.225-2
http://acquisition.gov/far/current/html/52_223_226.html

[Common] FPKIPA X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework, Version 3647 - 1.17, December 9, 2011
http://idmanagement.gov/documents/federal-pki-common-policy-framework-certificate-authority

[E-PACS] FICAM Personal Identity Verification (PIV) in Enterprise Physical Access Control Systems (E-PACS), Version 3.0, March 26, 2014
http://idmanagement.gov/documents/piv-e-pacs

[FBCA] FBCA X.509 Certificate Policy For Federal Bridge Certification Authority (FBCA), Version 2.25, December 9, 2011
http://idmanagement.gov/fbca-certificate-policy-page

[FIPS 201] Federal Information Processing Standard 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors
http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf

[FRTC] FIPS 201 Evaluation Program Functional Requirements and Test Cases
http://idmanagement.gov/ficam-testing-program-documents

[HSPD-12] Homeland Security Presidential Directive 12, August 27, 2004
https://www.dhs.gov/homeland-security-presidential-directive-12

[M-05-24] Office of Management and Budget (OMB) Memorandum M-05-24, August 5, 2005
http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf

[M-06-18] Office of Management and Budget (OMB) Memorandum M-06-18, June 30, 2006
http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-18.pdf

[M-11-11] OMB Memorandum M-11-11, February 3, 2011
http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf

[RFC 4530] IETF RFC 4530, “Lightweight Directory Access Protocol (LDAP) entry UUID Operational Attribute,” June 2006
http://www.ietf.org/rfc/rfc4530.txt

[Roadmap] FICAM Roadmap and Implementation Guidance, Version 2.0, December 2, 2011
http://idmanagement.gov/documents/ficam-roadmap-and-implementation-guidance

[Sect508] Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998
http://www.section508.gov/section508-laws

[SP800-73] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-73-3, Parts 1-3, February 2010
http://csrc.nist.gov/publications/nistpubs/800-73-3/sp800-73-3_PART1_piv-card-applic-namespace-date-model-rep.pdf

http://csrc.nist.gov/publications/nistpubs/800-73-3/sp800-73-3_PART2_piv-card-applic-card-common-interface.pdf

http://csrc.nist.gov/publications/nistpubs/800-73-3/sp800-73-3_PART3_piv-client-applic-programming-interface.pdf

[SP800-76] NIST SP 800-76-1, January 2007
http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf

[SP800-78] NIST SP 800-78-3, December 2010
http://csrc.nist.gov/publications/nistpubs/800-78-3/sp800-78-3.pdf

[SP800-96] NIST SP 800-96, September 2006
http://csrc.nist.gov/publications/nistpubs/800-96/SP800-96-091106.pdf

[SP800-116] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-116, November 2008
http://csrc.nist.gov/publications/nistpubs/800-116/SP800-116.pdf

[SP800-153] NIST SP 800-153, February 2012
http://csrc.nist.gov/publications/nistpubs/800-153/sp800-153.pdf

[TAA] Trade Agreement Act Certification FAR 52.225-6
http://acquisition.gov/far/current/html/52_223_226.html**[UL 294]** The Standard of Safety for Access Control System Units, UL Edition Number – 5, Date 01/29/1999, Type ULSTD
http://www.ul.com/global/eng/pages/offerings/industries/lifesafetyandsecurity/securityandsignaling/security/standards/

[UL 1076] The Standard of Safety for Proprietary Alarm Units, UL Edition Number – 5, Date 09/29/1995, Type ULSTD
http://www.ul.com/global/eng/pages/offerings/industries/lifesafetyandsecurity/securityandsignaling/security/standards/

[UL 1981] The Standard for Central-Station Automation Systems UL Edition Number -2, Date 06/30/2003, Type ULSTD
http://www.ul.com/global/eng/pages/offerings/industries/lifesafetyandsecurity/securityandsignaling/security/standards/

Appendix 1 Functional Requirements and Test Cases

1	Scoring Guidelines
	Security - A control directly impacting security of the system.
	Usability - A control impacting end user system usability. Does not directly impact security.
	Required - Must be present. Must work correctly: Red/Green.
	Optional - May be present. If present, it must work correctly: Red/Green. Not present: Yellow.

Products to be listed on the APL shall not have any tests scored RED. Products listed on the APL may have tests scored YELLOW.

		2	Requirements at Time of In-Person Registration In Accordance With [E-PACS] PIA-9	All tests use PKI-AUTH unless specifically noted. All tests using a CONTACT reader unless specifically noted.	Note all requirements sourced from [E-PACS] unless otherwise noted.	
Security/ Usability	**Required/ Optional**	**Test**	**Requirement**	**Test Case: Pass/Fail criteria**	**Requirement Source**	**Severity Level**
		2.1	**Signature Verification**			
Security	Required	2.1.1	Verify product’s ability to validate signatures in the certificates found in the certification path for a PIV credential.	Card 1: PIV Golden Registers successfully.	PIA-2 thru PIA-7	Sev-1
Security	Required	2.1.2	Verify product’s ability to validate signatures in the certificates found in the certification path for a PIV-I credential.	Card 2: PIV-I Golden Registers successfully	PIA-2 thru PIA-7	Sev-1
Security	Required	2.1.3	Verify product’s ability to recognize invalid signature on an intermediate CA in the certification path.	Card 1: (Golden PIV Card) w/PKI Path 1 fails to register successfully.	PAI-3.2, PIA-3.4, PIA-4, PIA-5	Sev-1
Security	Required	2.1.4	Verify product’s ability to recognize invalid signature on the End Entity certificate.	Card 5: invalid PIV/Card Auth Signer fails to register successfully.	PAI-3.2, PIA-3.4, PIA-4	Sev-1
Security	Required	2.1.5	Verify product’s ability to recognize certificate/private key mismatch.	Card 23: Certificate Private Key mismatch fails to register successfully.	PAI-3.2, PIA-3.4, PIA-4	Sev-1
		2.2	**Certificate Validity Periods**			

Security	Required	2.2.1	Verify product’s ability to reject a credential when *notBefore* date of the intermediate CA certificate is sometime in the future.	Card 1: (Golden PIV Card) w/PKI Path 2 fails to register successfully.	PIA-3.5, PIA-5	Sev-3
Security	Required	2.2.2	Verify product’s ability to reject a credential when *notAfterDate* of the End Entity Signing CA is sometime in the past.	Card 10: expired signing CA fails to register successfully.	PAI-3.2, PIA-3.4, PIA-4	Sev-2
Security	Required	2.2.3	Verify product’s ability to reject a credential when *notBefore* date of the End Entity certificate is sometime in the future.	Card 12: (Certs not yet valid) fails to register successfully.	PIA-3.5	Sev-3
Security	Required	2.2.4	Verify product’s ability to reject a credential when *notAfter* date of the intermediate certificate is sometime in the past.	Card 1: (Golden PIV Card) w/PKI Path 3 fails to register successfully.	PIA-3.5, PIA-5	Sev-1
Security	Required	2.2.5	Verify product’s ability to reject a credential when *notAfter* date of the End Entity certificate is sometime in the past.	Card 13: (Certs Expired) fails to register successfully.	PIA-3.5	Sev-1
		2.3	**Name Chaining**			
Security	Required	2.3.1	Verify product’s ability to reject a credential when common name portion of the issuer's name in the End Entity certificate does not match common name portion of subject's name in the previous intermediate certificate.	Card 1: (Golden PIV Card) w/PKI Path 4 fails to register successfully.	PIA-3.2, PIA-5	Sev-1
		2.4	**Basic Constraints Verification**			

Security	Required	2.4.1	Verify product's ability to recognize when the intermediate CA certificate is missing *basicConstraints* extension.	Card 1: (Golden PIV Card) w/PKI Path 5 fails to register successfully.	PIA-3.2, PIA-5	Sev-1
Security	Required	2.4.4	Verify product's ability to recognize when the first certificate in the path includes *basicConstraints* extension with a *pathLenConstraint* of 0 (this prevents additional intermediate certificates from appearing in the path). The first certificate is followed by the second intermediate CA certificate and an End Entity certificate.	Card 1: (Golden PIV Card) w/PKI Path 8 fails to register successfully.	PIA-3.2, PIA-5	Sev-1
Security	Required	2.4.5	Verify product’s ability to detect a mismatched SKID with the subject public key in the certificate.	Card 3: (SKID Mismatch Card) fails to register successfully.	PIA-3.2, PIA-5	Sev-3
		2.5	**Key Usage Verification**			
Security	Required	2.5.1	Verify product’s ability to recognize when the intermediate certificate includes a *keyUsage* extension in which *keyCertSign* is false.	Card 1: (Golden PIV Card) w/PKI Path 9 fails to register successfully.	PIA-3.2, PIA-5	Sev-1
Security	Required	2.5.3	Verify product’s ability to recognize when the intermediate certificate includes a *keyUsage* extension in which *crlSign* is false.	Card 1: (Golden PIV Card) w/PKI Path 11 fails to register successfully.	PIA-3.2, PIA-5	Sev-1
		2.6	**Certificate Policies**			

Security	Required	2.6.1	With the trust anchor set to Common Policy check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate path. The explicit policy will be set to PIV Hardware by the relying party solution.	Production PIV registers successfully.	PIA-3.2, PIA-5	Sev-1
Security	Required	2.6.2	With the trust anchor set to Common Policy check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate path. The explicit policy will be set by the relying party solution to an arbitrary value that is not present in the certificate path (e.g., OID value 1.2.3.4).	Production PIV fails to register.	PIA-3.2, PIA-5	Sev-1
Security	Required	2.6.3	With the trust anchor set so the certificate path requires trust across the Federal Bridge to the CertiPath Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate in a bridged trust environment. The explicit policy will be set to Medium Hardware by the relying party solution. Test Condition: production PIV passes.	Production PIV registers successfully.	PIA-3.2, PIA-5	Sev-2

Security	Required	2.6.4	With the trust anchor set so the certificate path requires trust across the Federal Bridge to the CertiPath Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate in a bridged trust environment. The explicit policy will be set to an arbitrary value that is not present in the certificate chain (e.g., OID value 1.2.3.4) by the relying party solution.	Production PIV fails to register.	PIA-3.2, PIA-5	Sev-2
Security	Required	2.6.5	With Common Policy anchor, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate - however, is present somewhere in the certificate path. The explicit policy will be set by the relying party solution to a value that is present in the certificate path, but does not map to the end entity certificate (e.g., High Hardware).	Production PIV fails to register.	PIA-3.2, PIA-5	Sev-1
Security	Required	2.6.8	With required policy set to 2.16.840.1.101.3.2.1.48.11 (test id-fpki-common-authentication), verify product’s ability to process a path that includes a *policyConstraints* extension with *inhibitPolicyMapping* set to 0 which invalidates the ICAM Test Bridge to ICAM Root CA policy mappings.	Card 1: (Golden PIV Card) w/PKI Path 12 fails to register successfully.	PIA-3.2, PIA-5	Sev-2
		2.7	**Generalized Time**			

Security	Required	2.7.1	Verify product's ability to process valid use of generalized time post year 2049 in the path.	Card 1: (Golden PIV Card) w/PKI Path 24 registers successfully.	PIA-3.2, PIA-5	Sev-3
Security	Required	2.7.2	Verify product's ability to process invalid use of generalized time before year 2049 in the path.	Card 1: (Golden PIV Card) w/PKI Path 25 fails to register successfully.	PIA-3.2, PIA-5	Sev-3
		2.8	**Name Constraints**			
Security	Required	2.8.1	The system recognizes when the intermediate certificate includes a *nameConstraints* extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree.	Card 1: (PIV Golden) registers successfully.	PIA-3.2, PIA-5	Sev-1
Security	Required	2.8.2	The system recognizes when the intermediate certificate includes a *nameConstraints* extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls outside that subtree.	Card 1: (Golden PIV Card) w/PKI Path 13 fails to register successfully.	PIA-3.2, PIA-5	Sev-1
Security	Required	2.8.3	The system recognizes when the intermediate certificate includes a *nameConstraints* extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree and *subjectAltName* with a DN that falls outside that subtree.	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.** Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PIA-3.2, PIA-5	Sev-2

		2.9	**Certificate Revocation Tests (CRL)**			
Security	Required	2.9.1	The system recognizes when no revocation information is available for the End Entity certificate	Card 1: (Golden PIV Card) w/PKI Path 15 fails to register successfully.	PIA-3.5, PIA-5, PIA-7	Sev-1
Security	Required	2.9.2	The system recognizes when a second intermediate CA certificate is revoked.	Card 1: (Golden PIV Card) w/PKI Path 16 fails to register successfully.	PIA-3.5, PIA-5, PIA-7	Sev-1
Security	Required	2.9.3	The system recognizes when the End Entity certificate is revoked.	Card 24: (Revoked status) fails to register successfully.	PIA-3.5, PIA-5, PIA-7	Sev-1
Security	Required	2.9.4	The system recognizes when a certificate in the path links to a CRL issued by a CA other than that which issued the certificate.	Card 1: (Golden PIV Card) w/PKI Path 18 fails to register successfully.	PIA-3.5, PIA-5, PIA-7	Sev-1
Security	Required	2.9.5	The system recognizes when a certificate in the path points to a CRL with an expired *nextUpdate* value (an expired CRL).	Card 1: (Golden PIV Card) w/PKI Path 19 fails to register successfully.	PIA-3.5, PIA-5, PIA-7	Sev-1
Security	Required	2.9.6	The system recognizes when a certificate in the path points to a CRL with a *notBefore* Date in the future.	Card 1: (Golden PIV Card) w/PKI Path 20 fails to register successfully.	PIA-3.5, PIA-5, PIA-7	Sev-3
Security	Required	2.9.7	The system recognizes when a certificate in the path has an incorrect CRL distribution point.	Card 1: (Golden PIV Card) w/PKI Path 21 fails to register successfully.	PIA-3.5, PIA-5, PIA-7	Sev-1
Security	Required	2.9.8	The system recognizes when the CRL has an invalid signature.	Card 1: (Golden PIV Card) w/PKI Path 17 fails to register successfully.	PIA-3.5, PIA-5, PIA-7	Sev-1

Security	Required	2.9.9	The system recognizes when an incorrectly formatted CRL is present in the path.	Card 1: (Golden PIV Card) w/PKI Path 34 fails to register successfully.	PIA-3.5, PIA-5, PIA-7	Sev-2
Security	Required	2.9.10	The system recognizes when an invalid CRL signer is in the path.	Card 1: (Golden PIV Card) w/PKI Path 36 fails to register successfully.	PIA-3.5, PIA-5, PIA-7	Sev-1
		2.10	**CHUID Verification**			
Security	Required	2.10.1	The system recognizes when the CHUID signature is invalid and does not verify.	Card 4: (Invalid CHUID Signature) fails to register successfully.	PIA-3.2, PIA-4	Sev-1
Security	Required	2.10.2	The system recognizes when the CHUID signer certificate is expired.	Card 9: (Expired CHUID signer) fails to register successfully.	PIA-3.6, PIA-5	Sev-2
Security	Required	2.10.3	The system recognizes when the CHUID is expired.	Card 14: (Card Expired) fails to register successfully.	PIA-3.6	Sev-1
Security	Required	2.10.4	The system recognizes when the FASC-N in the CHUID does not equal the FASC-N in the PIV Auth Cert.	Card 15: (FASC-N in CHUID !=) fails to register successfully.	PIA-3.2; [SP800-73], Part 1, §3.1.2	Sev-2
Security	Required	2.10.5	The system recognizes when the UUID in the CHUID does not equal the UUID in the PIV-I Auth Cert.	Card 19: (UUID in CHUID !=) fails to register successfully.	PIA-3.2; [SP800-73], Part 1, §3.3	Sev-2
Security	Required	2.10.6	The system recognizes when the PKI-AUTH certificate expires after the CHUID expiration date.	Card 11: (PKI-AUTH Cert after CHUID) fails to register successfully.	[FIPS 201]; [FBCA] §6.3.2, Appendix A (10) & (11)	Sev-1

Security	Required	2.10.7	The system recognizes when the CHUID expiration date is after the CHUID signer certificate expiration date.	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.** Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	[FIPS 201]; [FBCA] §6.3.2, Appendix A (10) & (11)	Sev-2
Security	Required	2.10.8	The system recognizes when an intermediate certificate in the CHUID signer certificate path is expired.	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.** Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	[FIPS 201]; [FBCA] §6.3.2, Appendix A (10) & (11)	Sev-2
Security	Required	2.10.9	The system recognizes when an intermediate certificate in the CHUID signer certificate path is revoked.	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.** Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	[FIPS 201]; [FBCA] §6.3.2, Appendix A (10) & (11)	Sev-1
		2.11	**Facial Image Verification**	**If Facial Image is Supported, tests in this section are Required.**		

Security	Required	2.11.1	The system recognizes when the Facial Image signature is invalid and does not verify.	Card 6: (bad photo signature) fails to register successfully.	PIA-3.2, PIA-4	Sev-1
		2.12	**Copied Containers**			
Security	Required	2.12.1	The system recognizes when the FASC-N in the PKI-CAK certificate does not equal the FASC-N in the PIV Auth Cert.	Card 16: (FASC-N in PKI-CAK Cert !=) fails to register successfully.	PIA-3.2; [SP800-73], Part 1, §3.1.2	Sev-1
Security	Required	2.12.2	The system recognizes when the UUID in the PKI-CAK certificate does not equal the UUID in the PIV-I Auth Cert.	Card 20: (UUID in PKI-CAK Cert !=) fails to register successfully.	PIA-3.2; [SP800-73], Part 1, §3.1.2	Sev-1
Security	Required	2.12.3	The system recognizes when the FASC-N in the Facial Image does not equal the FASC-N in the PIV Auth Cert.	Card 17: (FASC-N in Facial Image !=) fails to register successfully.	PIA-3.2; [SP800-73], Part 1, §3.1.2	Sev-1
Security	Required	2.12.4	The system recognizes when the UUID in the Facial Image does not equal the UUID in the PIV-I Auth Cert.	Card 21: (UUID in Facial Image !=) fails to register successfully.	PIA-3.2; [SP800-73], Part 1, §3.1.2	Sev-1
		2.13	**FINGERPRINT Verification**	**If BIO Authentication Method is Supported at time of registration, tests in this section are Required. If content signer certificate is from CHUID, Section 2.10 is Required.**		
Security	Required	2.13.1	The system recognizes when the Fingerprint signature is invalid and does not verify (using CHUID content signer certificate).	Card 7: (bad fingerprint signature) fails to register successfully.	PIA-3.2, PIA-4	Sev-1

Security	Required	2.13.2	The system recognizes when the Fingerprint signature is invalid and does not verify (using biometric object signer certificate).	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.** Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PIA-3.2, PIA-3.4, PIA-3.5, PIA-3.6, PIA-4, PIA-5	Sev-1
Security	Required	2.13.3	Verify Product's ability to accept a valid credential with a matching fingerprint.	A good credential is presented to the system with a valid fingerprint object on card. System is presented correct bearer's fingerprint. Registration succeeds.	PIA-3 thru PIA-7	Sev-1
Security	Required	2.13.4	Verify Product's ability to reject a valid credential with a non-matching fingerprint.	A good credential is presented to the system with a valid fingerprint object on card. System is presented incorrect bearer's fingerprint. Registration fails.	PIA-3.3	Sev-1
Security	Required	2.13.5	The system recognizes when the FASC-N in the Fingerprint does not equal the FASC-N in the PIV Auth Cert.	Card 18: (FASC-N in Fingerprint !=) fails to register successfully.	PIA-3.2; [SP800-73], Part 1, §3.1.2	Sev-1
Security	Required	2.13.6	The system recognizes when the UUID in the Fingerprint does not equal the UUID in the PIV-I Auth Cert	Card 22: (UUID in Fingerprint !=) fails to register successfully.	PIA-3.2; [SP800-73], Part 1, §3.1.2	Sev-1
		2.14	**Security Object Verification**	**If Security Object is Supported, tests in this section are Required.**		

Security	Required	2.14.1	The system recognizes when the Security Object signature is invalid and does not verify.	Card 8: (bad security object signature) fails to register successfully.	PIA-3.4, PIA-4, PIA-5	Sev-3
		2.15	**OCSP Response Checking**			
Security	Required	2.15.1	The system successfully validates a good credential using an OCSP response with a good signature	Card 1: Golden PIV registers successfully.	PIA-3.2, PIA-3.5	Sev-1
Security	Required	2.15.2	Validation fails using an OCSP Responder with an expired signature certificate for a good card.	Card 1: Golden PIV w/PKI Path 37 fails to register successfully.	PIA-3.2 PIA-3.5, PIA-3.6	Sev-2
Security	Required	2.15.3	Validation succeeds using an OCSP Responder with a revoked signature certificate for a good card with PKIX_OCSP_NOCHECK present.	Card 1: Golden PIV w/PKI Path 38 registers successfully.	PIA-3.2, PIA-3.5	Sev-3
Security	Required	2.15.4	Validation fails using an OCSP Responder with a revoked signature certificate for a good card without PKIX_OCSP_NOCHECK present.	Card 1: Golden PIV w/PKI Path 39 fails to register successfully.	PIA-3.2, PIA-3.5, PIA-3.6	Sev-2
Security	Required	2.15.5	Validation fails using an OCSP Responder with a signature certificate containing an invalid signature for a good card.	Card 1: Golden PIV w/PKI Path 40 fails to register successfully.	PIA-3.2, PIA-4	Sev-1
		2.16	**Interoperability Testing**	**Tests in this section use a variety of dual interface and dual chip production PIV and PIV-I cards in the system.**		

Usability	Required	2.16.1	Various valid PIV (including CAC) and PIV-I cards can be individually registered using PKI-AUTH method.	PIV (including CAC) and PIV-I cards register successfully.	PIA-6	Sev-1
		2.17	**Cryptography Testing**			
Security	Required	2.17.2	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (2048).	NIST card#1 registers successfully.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5	Sev-1
Security	Required	2.17.3	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (3072).	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.** Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5	Sev-1
Security	Optional	2.17.5	Verify Product's ability to validate signatures using RSASSA-PSS (2048).	NIST card#2 registers successfully.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5	Sev-3

Security	Optional	2.17.6	Verify Product's ability to validate signatures using RSASSA-PSS (3072).	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.** Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5	Sev-3
Security	Required	2.17.7	Verify Product’s ability to validate signatures using ECDSA (P-256).	NIST card#4 registers successfully.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5	Sev-1
Security	Optional	2.17.8	Verify Product’s ability to validate signatures using ECDSA (P-384).	NIST card#5 registers successfully.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5	Sev-3
Security	Required	2.17.10	Verify Product’s ability to validate signatures using SHA-256.	NIST card#1 registers successfully.	[SP800-78] Table 3-7; [Common] §6.1.5	Sev-1
Security	Optional	2.17.11	Verify Product’s ability to validate signatures using SHA-384.	NIST card#5 registers successfully.	[SP800-78] Table 3-7; [Common] §6.1.5	Sev-3

Security	Required	2.17.12	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (2048) w/exponent of 65,537.	NIST card#1 registers successfully.	[SP800-78] Table 3-2	Sev-1
Security	Optional	2.17.13	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (2048) w/exponent of 2^256-1.	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.** Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	[SP800-78] Table 3-2	Sev-3
Security	Required	2.17.14	Verify product’s ability to validate signatures using RSA 4096 in the path.	Card 1: (Golden PIV Card) w/PKI Path 35 registers successfully.	Derived from [SP800-78] Table 3-2	Sev-3
		2.18	**Discovery Object & PIN Usage Policy**	**All tests use PKI-Auth.** **§2.18.x Discovery Object & PIN Usage Policy will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.**		
Security	Required	2.18.1	Discovery object not present. Confirm E-PACS is using Application PIN.	Use Card 25 and enter invalid PIN (e.g., 999999). Registration fails. Confirm PIV App PIN retry counter is decremented by one.	[SP800-73] Part 1, §3.2.6, §5.1	Sev-2

Security	Required	2.18.2	Discovery object not present. Confirm E-PACS is using the Application PIN.	Use Card 25 and enter PIV App PIN. Registration succeeds. Confirm PIV App PIN retry counter is reset to 5.	[SP800-73] Part 1, §3.2.6, §5.1	Sev-2
Security	Required	2.18.3	Discovery object present and set for PIV App PIN only. Confirm E-PACS is using the Application PIN.	Use Card 26 and enter invalid PIN (e.g., 999999). Registration fails. Confirm PIV App PIN retry counter is decremented by one.	[SP800-73] Part 1, §3.2.6, §5.1	Sev-2
Security	Required	2.18.4	Discovery object is present and set for PIV App PIN only. Confirm E-PACS is using the Application PIN.	Use Card 26 and enter PIV App PIN. Registration succeeds. Confirm PIV App PIN retry counter is reset to 5.	[SP800-73] Part 1, §3.2.6, §5.1	Sev-2
Security	Required	2.18.5	Discovery object is present. PIV App and Global PINs are available. PIV App PIN is primary. Confirm E-PACS is using the Application PIN.	Use Card 27 and enter invalid PIV App PIN (e.g., 999999). Registration fails. Confirm PIV App PIN retry counter is decremented by one (from 5 to 4). Confirm Global PIN retry counter remains at 5.	[SP800-73] Part 1, §3.2.6, §5.1	Sev-2

Security	Optional	2.18.6	Discovery object is present. PIV App and Global PINs are available. PIV App PIN is primary. Confirm E-PACS is using the Global PIN.	Use Card 27 and enter invalid Global PIN (e.g., 999999). Registration fails. Confirm PIV App PIN retry counter remains at 4. Confirm Global PIN retry counter is decremented by one (from 5 to 4).	[SP800-73] Part 1, §3.2.6, §5.1	Sev-2
Security	Required	2.18.7	Discovery object is present. PIV App and Global PINs are available. PIV App PIN is primary. Confirm E-PACS is using the Application PIN.	Use Card 27 and enter PIV App PIN. Registration succeeds. Confirm PIV App PIN retry counter reset to 5. Confirm Global PIN retry counter remains at 4.	[SP800-73] Part 1, §3.2.6, §5.1	Sev-2
Security	Optional	2.18.8	Discovery object is present. PIV App and Global PINs are available. PIV App PIN is primary. Confirm E-PACS is using the Global PIN.	Use Card 27 and enter Global PIN. Registration succeeds. Confirm PIV App PIN retry counter remains at 5. Confirm Global PIN retry counter reset to 5.	[SP800-73] Part 1, §3.2.6, §5.1	Sev-2

Security	Required	2.18.9	Discovery object is present. PIV App and Global PINs are available. Global PIN is primary. Confirm E-PACS is using the Application PIN.	Use Card 28 and enter invalid PIV App PIN (e.g., 999999). Registration fails. Confirm PIV App PIN retry counter is decremented by one (from 5 to 4). Confirm Global PIN retry counter remains at 5.	[SP800-73] Part 1, §3.2.6, §5.1	Sev-2
Security	Optional	2.18.10	Discovery object is present. PIV App and Global PINs are available. Global PIN is primary. Confirm E-PACS is using the Global PIN.	Use Card 28 and enter invalid Global PIN (e.g., 999999). Registration fails. Confirm PIV App PIN retry counter remains at 4. Confirm Global PIN retry counter is decremented by one (from 5 to 4).	[SP800-73] Part 1, §3.2.6, §5.1	Sev-2
Security	Required	2.18.11	Discovery object is present. PIV App and Global PINs are available. Global PIN is primary. Confirm E-PACS is using the Application PIN.	Use Card 28 and enter PIV App PIN. Registration succeeds. Confirm PIV App PIN retry counter reset to 5. Confirm Global PIN retry counter is reset to 5.	[SP800-73] Part 1, §3.2.6, §5.1	Sev-2

		3	**Dual Chip Card, time of registration**	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.** Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	**[FIPS 201]**	
		3.1	**CHUID Verification (Contactless chip on a 2 chip card)**	**These tests are run using a contactless reader**		
Security	Required	3.1.1	The system recognizes when the CHUID signature is invalid and does not verify.	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.** Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PIA-3.2, PIA-4	Sev-1
Security	Required	3.1.2	The system recognizes when the CHUID signer certificate is expired.	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.** Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PIA-3.6, PIA-5	Sev-2

Security	Required	3.1.3	The system recognizes when the CHUID is expired.	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.** Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PIA-3.6	Sev-1
Security	Required	3.1.4	The system recognizes when the PKI-CAK certificate expires after the CHUID expiration date.	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.** Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	[FIPS 201]; [FBCA] §6.3.2, Appendix A (10) & (11)	Sev-1
		3.2	**Copied Containers**			
Security	Required	3.2.1	The system recognizes when the FASC-N in the CHUID does not equal the FASC-N in the PIV PKI-CAK Cert.	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.** Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PIA-3.2; [SP800-73], Part 1, §3.1.2	Sev-2

Security	Required	3.2.2	The system recognizes when the UUID in the CHUID does not equal the UUID in the PIV-I PKI-CAK Cert.	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.** Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PIA-3.2; [SP800-73], Part 1, §3.1.2	Sev-2
		3.3	**Signature Verification (Contactless chip on a 2 chip card)**	**These tests are run using a contactless reader. PKI-CAK mode is used for all tests.**		
Security	Required	3.3.1	Verify product’s ability to validate signatures in the certificates found in the certification path for a PIV credential.	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.** Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PIA-2 thru PIA-7	Sev-1

Security	Required	3.3.2	Verify product's ability to validate signatures in the certificates found in the certification path for a PIV-I credential.	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.** Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PIA-2 thru PIA-7	Sev-1
Security	Required	3.3.3	Verify product's ability to recognize invalid signature on an intermediate CA in the certification path.	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.** Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PAI-3.2, PIA-3.4, PIA-4, PIA-5	Sev-1
Security	Required	3.3.4	Verify product's ability to recognize invalid signature on the End Entity certificate.	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.** Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PAI-3.2, PIA-3.4, PIA-4	Sev-1

Security	Required	3.3.5	Verify product's ability to recognize certificate/private key mismatch.	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.** Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PAI-3.2, PIA-3.4, PIA-4	Sev-1
		4	**Requirements for Automated Provisioning In Accordance With [E-PACS] PIA-8**	.		
		4.1	**Dual Interface Chip Card**			
Security	Optional	4.1.1	The E-PACS shall accept automated provisioning from a source it trusts and that complies with the security requirements described in the detailed guidance of PIA-8.	Perform design analysis of automated provisioning functionality of the solution.	PIA-8; [Roadmap], §9.2.3.1 including Figure 94	Sev-2
Security	Optional	4.1.2	The E-PACS shall accept automated de-provisioning from a source it trusts and that complies with the security requirements described in PIA-3.5 and PIA-3.6.	Perform design analysis of automated de-provisioning functionality of the solution.	PIA-8, PIA-3.5, PIA-3.6; [Roadmap], §9.2.3.1 including Figure 94	Sev-2

		4.2	**Dual Chip Card**	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.** Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	[FIPS 201]	
Security	Optional	4.2.1	The E-PACS shall accept automated provisioning of the contactless CAK from a source it trusts and that complies with the security requirements described in the detailed guidance of PIA-8.	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.** Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PIA-8; [Roadmap], §9.2.3.1 including Figure 94	Sev-2
Security	Optional	4.2.2	The E-PACS shall accept automated de-provisioning of the contactless CAK from a source it trusts and that complies with the security requirements described in PIA-3.5 and PIA-3.6.	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.** Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PIA-8, PIA-3.5, PIA-3.6; [Roadmap], §9.2.3.1 including Figure 94	Sev-2

		5	Authentication at Time of Access Test Cases	All tests use PKI-AUTH unless specifically noted.		
		5.1	**Signature Verification**			
Security	Required	5.1.1	Verify product's ability to validate signatures in the certificates found in the certification path for a PIV credential.	Card 1: PIV Golden Receives an access grant Successfully.	PIA-2 thru PIA-7	Sev-1
Security	Optional	5.1.2	Verify product's ability to validate signatures in the certificates found in the certification path for a PIV-I credential.	Card 2: PIV-I Golden Receives an access grant Successfully.	PIA-2 thru PIA-7	Sev-1
Security	Required	5.1.3	Verify product's ability to recognize invalid signature on an intermediate CA in the certification path.	Card 1: (Golden PIV Card) w/PKI Path 1 fails to receive an access grant.	PAI-3.2, PIA-3.4, PIA-4, PIA-5	Sev-1
Security	Required	5.1.4	Verify product's ability to recognize invalid signature on the End Entity certificate.	Card 5: invalid PIV/Card Auth Signer fails to receive an access grant. This shall not be tested when the solution leverages a cached copy of the public key extracted at time of registration for signature verification at time of access.	PAI-3.2, PIA-3.4, PIA-4	Sev-1
Security	Required	5.1.5	Verify product's ability to recognize manipulated keys.	Card 23: Manipulated key fails to receive an access grant.	PAI-3.2, PIA-3.4, PIA-4	Sev-1

Security	Required	5.1.6	Verify product’s ability to recognize public key from card does not match public key previously registered to the system.	Card 3: Substituted keypair in PKI-AUTH certificate fails to receive an access grant. This shall not be tested when the solution leverages a cached copy of the public key extracted at time of registration for signature verification at time of access.	PIA-3.2	Sev-1
		5.2	**Certificate Validity Periods**			
Security	Required	5.2.1	Verify product’s ability to reject a credential when *notBefore* date of the intermediate CA certificate is sometime in the future.	Card 1: (Golden PIV Card) fails access grant w/PKI Path 2.	PIA-3.5, PIA-5	Sev-3
Security	Required	5.2.2	Verify product’s ability to reject a credential when *notBefore* date of the End Entity certificate is sometime in the future.	Card 12: (Certs not yet valid) access grant fails. This shall not be tested when the solution leverages a cached copy of the public key extracted at time of registration for signature verification at time of access.	PIA-3.5	Sev-2
Security	Required	5.2.3	Verify product’s ability to reject a credential when *notAfter* date of the intermediate certificate is sometime in the past.	Card 1: (Golden PIV Card) fails access grant w/PKI Path 3.	PIA-3.5, PIA-5	Sev-1

Security	Required	5.2.4	Verify product’s ability to reject a credential when *notAfter* date of the End Entity certificate is sometime in the past.	Card 13: (Certs Expired) access grant fails. This shall not be tested when the solution leverages a cached copy of the public key extracted at time of registration for signature verification at time of access.	PIA-3.5	Sev-1
		5.3	**Name Chaining**			
Security	Required	5.3.1	Verify product’s' ability to reject a credential when common name portion of the issuer's name in the End Entity certificate does not match common name portion of subject's name in the previous intermediate certificate.	Card 1: (Golden PIV Card) fails access grant w/PKI Path 4.	PIA-3.2, PIA-5	Sev-1
		5.4	**Basic Constraints Verification**			
Security	Required	5.4.1	Verify product's ability to recognize when the intermediate CA certificate is missing *basicConstraints* extension.	Card 1: (Golden PIV Card) fails access grant w/PKI Path 5.	PIA-3.2, PIA-5	Sev-1
Security	Required	5.4.4	Verify product's ability to recognize when the first certificate in the path includes *basicConstraints* extension with a *pathLenConstraint* of 0 (this prevents additional intermediate certificates from appearing in the path). The first certificate is followed by the second intermediate CA certificate and an End Entity certificate.	Card 1: (Golden PIV Card) fails access grant w/PKI Path 8.	PIA-3.2, PIA-5	Sev-1

Security	Required	5.4.5	Verify product's ability to detect a mismatched SKID with the subject public key in the certificate.	Card 1: (Golden PIV Card) w/PKI Path 32 receives access denied.	PIA-3.2, PIA-5	Sev-3
		5.5	**Key Usage Verification**			
Security	Required	5.5.1	Verify product's ability to recognize when the intermediate certificate includes a *keyUsage* extension in which *keyCertSign* is false	Card 1: (Golden PIV Card) fails access grant w/PKI Path 9	PIA-3.2, PIA-5	Sev-1
Security	Required	5.5.3	Verify product's ability to recognize when the intermediate certificate includes a *keyUsage* extension in which *crlSign* is false.	Card 1: (Golden PIV Card) fails access grant w/PKI Path 11.	PIA-3.2, PIA-5	Sev-1
		5.6	**Certificate Policies**			
Security	Required	5.6.1	With the trust anchor set to Common Policy check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate path. The explicit policy will be set to PIV Hardware by the relying party solution.	Production PIV receives access grant.	PIA-3.2, PIA-5	Sev-1

Security	Required	5.6.2	With the trust anchor set to Common Policy check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate path. The explicit policy will be set by the relying party solution to an arbitrary value that is not present in the certificate path (e.g., OID value 1.2.3.4).	Production PIV receives access denied.	PIA-3.2, PIA-5	Sev-1
Security	Required	5.6.3	With the trust anchor set so the certificate path requires trust across the Federal Bridge to the CertiPath Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate in a bridged trust environment. The explicit policy will be set to Medium Hardware by the relying party solution. Test Condition: production PIV passes.	Production PIV receives access grant.	PIA-3.2, PIA-5	Sev-2
Security	Required	5.6.4	With the trust anchor set so the certificate path requires trust across the Federal Bridge to the CertiPath Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate in a bridged trust environment. The explicit policy will be set to an arbitrary value that is not present in the certificate chain (e.g., OID value 1.2.3.4) by the relying party solution.	Production PIV receives access denied.	PIA-3.2, PIA-5	Sev-2

Security	Required	5.6.5	With Common Policy anchor, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate - however, is present somewhere in the certificate path. The explicit policy will be set by the relying party solution to a value that is present in the certificate path, but does not map to the end entity certificate (e.g., High Hardware).	Production PIV receives access denied.	PIA-3.2, PIA-5	Sev-1
Security	Required	5.6.8	With required policy set to 2.16.840.1.101.3.2.1.48.11 (test id-fpki-common-authentication), verify product's ability to process a path that includes a *policyConstraints* extension with *inhibitPolicyMapping* set to 0 which invalidates the ICAM Test Bridge to ICAM Root CA policy mappings.	Card 1: (Golden PIV Card) fails access grant w/PKI Path 12.	PIA-3.2, PIA-5	Sev-2
		5.7	**Generalized Time**			
Security	Required	5.7.1	Verify product's ability to process valid use of generalized time post year 2049 in the path.	Card 1: (Golden PIV Card) w/PKI Path 24 receives access grant.	PIA-3.2, PIA-5	Sev-3
Security	Required	5.7.2	Verify product's ability to process invalid use of generalized time before year 2049 in the path.	Card 1: (Golden PIV Card) w/PKI Path 25 denied access.	PIA-3.2, PIA-5	Sev-3
		5.8	**Name Constraints**			

Security	Required	5.8.1	The system recognizes when the intermediate certificate includes a *nameConstraints* extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree.	Card 1: (PIV Golden) access grant succeeds	PIA-3.2, PIA-5	Sev-1
Security	Required	5.8.2	The system recognizes when the intermediate certificate includes a *nameConstraints* extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls outside that subtree.	Card 1: (Golden PIV Card) fails access grant w/PKI Path 13.	PIA-3.2, PIA-5	Sev-1
Security	Required	5.8.3	The system recognizes when the intermediate certificate includes a *nameConstraints* extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree and *subjectAltName* with a DN that falls outside that subtree.	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.** Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PIA-3.2, PIA-5	Sev-2
		5.9	**Certificate Revocation Tests (CRL)**			
Security	Required	5.9.1	The system recognizes when no revocation information is available for the End Entity certificate.	Card 1: (Golden PIV Card) fails access grant w/PKI Path 15.	PIA-3.5, PIA-5, PIA-7	Sev-1
Security	Required	5.9.2	The system recognizes when a second intermediate CA certificate is revoked.	Card 1: (Golden PIV Card) fails access grant w/PKI Path 16.	PIA-3.5, PIA-5, PIA-7	Sev-1

Security	Required	5.9.3	The system recognizes when the End Entity certificate is revoked.	No longer tested. Chasing CDP from the certificate on the card at time of access should never happen. CDP should only be trusted based on registration process. Card 24: Revoked status.	PIA-3.5, PIA-5, PIA-7	Sev-1
Security	Required	5.9.4	The system recognizes when the CRL has an invalid signature.	Card 1: (Golden PIV Card) fails access grant w/PKI Path 17.	PIA-3.5, PIA-5, PIA-7	Sev-1
Security	Required	5.9.5	The system recognizes when a certificate in the path links to a CRL issued by a CA other than that which issued the certificate.	Card 1: (Golden PIV Card) fails access grant w/PKI Path 18.	PIA-3.5, PIA-5, PIA-7	Sev-1
Security	Required	5.9.6	The system recognizes when a certificate in the path has an expired *nextUpdate* value (an expired CRL).	Card 1: (Golden PIV Card) fails access grant w/PKI Path 19.	PIA-3.5, PIA-5, PIA-7	Sev-1
Security	Required	5.9.7	The system recognizes when a certificate in the path points to a CRL with a *notBefore* Date in the future.	Card 1: (Golden PIV Card) fails access grant w/PKI Path 20.	PIA-3.5, PIA-5, PIA-7	Sev-3
Security	Required	5.9.8	The system recognizes when a certificate in the path has an incorrect CRL distribution point.	Card 1: (Golden PIV Card) fails access grant w/PKI Path 21.	PIA-3.5, PIA-5, PIA-7	Sev-1
		5.11	**Facial Image Verification**	**If showing facial image as part of an access transaction is Supported, tests in this section are Required.**		

Security	Required	5.11.1	The system recognizes when the Facial Image signature is invalid and does not verify.	Card 6: (bad photo signature) fails access grant.	PIA-3, PIA-3.2, PIA-3.3, PIA-4	Sev-1
		5.12	**FINGERPRINT Verification**	**If BIO Authentication Method is Supported, tests in this section are Required.**		
Security	Required	5.12.1	The system recognizes when the Fingerprint signature is invalid and does not verify (using CHUID content signer certificate).	Card 7: (bad fingerprint signature) access grant fails.	PIA-3, PIA-3.2, PIA-3.3, PIA-4	Sev-1
Security	Required	5.12.2	The system recognizes when the Fingerprint signature is invalid and does not verify (using biometric object signer certificate).	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.** Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PIA-3.2, PIA-3.4, PIA-3.5, PIA-3.6, PIA-4, PIA-5	Sev-1
Security	Required	5.12.3	Verify Product's ability to accept a valid credential with a matching fingerprint.	A good credential is presented to the system with a valid fingerprint object on card. System is presented correct bearer's fingerprint. Access is granted.	PIA-3 thru PIA-7	Sev-1

Security	Required	5.12.4	Verify Product's ability to reject a valid credential with a non-matching fingerprint.	A good credential is presented to the system with a valid fingerprint object on card. System is presented incorrect bearer's fingerprint. Access grant fails.	PIA-3.3	Sev-1
		5.13	**Security Object Verification**	**If Security Object is Supported, tests in this section are Required.**		
Security	Required	5.13.1	The system recognizes when the Security Object signature is invalid and does not verify.	Card 8: (bad security object signature) access grant fails.	PIA-3.4, PIA-4, PIA-5	Sev-3
		5.14	**OCSP Response Checking**			
Security	Required	5.14.1	The system successfully validates a good credential using an OCSP response with a good signature.	Card 1: Golden PIV is granted access.	PIA-3.2, PIA-3.5	Sev-1
Security	Required	5.14.2	Validation fails using an OCSP Responder with an expired signature certificate for a good card.	Card 1: Golden PIV w/PKI Path 37 access is denied.	PIA-3.2 PIA-3.5, PIA-3.6	Sev-2
Security	Required	5.14.3	Validation succeeds using an OCSP Responder with a revoked signature certificate for a good card with PKIX_OCSP_NOCHECK present.	Card 1: Golden PIV w/PKI Path 38 is granted access.	PIA-3.2, PIA-3.5	Sev-3
Security	Required	5.14.4	Validation fails using an OCSP Responder with a revoked signature certificate for a good card without PKIX_OCSP_NOCHECK present.	Card 1: Golden PIV w/PKI Path 39 access is denied.	PIA-3.2, PIA-3.5, PIA-3.6	Sev-2

Security	Required	5.14.5	Validation fails using an OCSP Responder with a signature certificate containing an invalid signature for a good card.	Card 1: Golden PIV w/PKI Path 40 access is denied.	PIA-3.2, PIA-4	Sev-1
		5.15	**Interoperability Testing**	**Tests in this section attempt to use a variety of dual interface production PIV and PIV-I cards in the system.**		
Usability	Required	5.15.1	Various valid PIV (including CAC) and PIV-I cards are granted access using PKI-AUTH method.	PIV (including CAC) and PIV-I cards are granted access.	PIA-6	Sev-1
		5.16	**Cryptography testing**			

Security	Required	5.16.2	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (2048).	NIST card#1 is granted access.	[SP800-78] Table 3-1;
					[SP800-78] Table 3-3;
					[Common] §6.1.5
						Sev-1

Security	Required	5.16.3	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (3072).	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.**
				Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.
					[SP800-78] Table 3-1;
					[SP800-78] Table 3-3;
					[Common] §6.1.5
						Sev-1

Security	Optional	5.16.5	Verify Product's ability to validate signatures using RSASSA-PSS (2048).	NIST card#2 is granted access.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5	Sev-3
Security	Optional	5.16.6	Verify Product's ability to validate signatures using RSASSA-PSS (3072).	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.** Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5	Sev-3
Security	Required	5.16.7	Verify Product’s ability to validate signatures using ECDSA (P-256).	NIST card#4 is granted access.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5	Sev-1
Security	Optional	5.16.8	Verify Product’s ability to validate signatures using ECDSA (P-384).	NIST card#5 is granted access.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5	Sev-3

Security	Required	5.16.10	Verify Product’s ability to validate signatures using SHA-256.	NIST card#1 is granted access.	[SP800-78] Table 3-7; [Common] §6.1.5	Sev-1
Security	Optional	5.16.11	Verify Product’s ability to validate signatures using SHA-384.	NIST card#5 is granted access.	[SP800-78] Table 3-7; [Common] §6.1.5	Sev-3
Security	Required	5.16.12	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (2048) w/exponent of 65,537.	NIST card#1 is granted access.	[SP800-78] Table 3-2	Sev-1
Security	Optional	5.16.13	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (2048) w/exponent of 2^256-1.	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.** Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	[SP800-78] Table 3-2	Sev-3
Security	Required	5.16.14	Verify product’s ability to validate signatures using RSA 4096 in the path.	Card 1: (Golden PIV Card) w/PKI Path 35 is granted access.		Sev-3

		5.17	**Discovery Object & PIN Usage Policy**	**All tests use PKI-Auth.** **§5.17.x Discovery Object & PIN Usage Policy will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.**		
Security	Required	5.17.1	Discovery object not present. Confirm E-PACS is using Application PIN.	Use Card 25 and enter invalid PIN (e.g., 999999). Registration fails. Confirm PIV App PIN retry counter is decremented by one.	[SP800-73] Part 1, §3.2.6, §5.1	Sev-2
Security	Required	5.17.2	Discovery object not present. Confirm E-PACS is using the Application PIN.	Use Card 25 and enter PIV App PIN. Access is granted. Confirm PIV App PIN retry counter is reset to 5.	[SP800-73] Part 1, §3.2.6, §5.1	Sev-2
Security	Required	5.17.3	Discovery object present and set for PIV App PIN only. Confirm E-PACS is using the Application PIN.	Use Card 26 and enter invalid PIN (e.g., 999999). Registration fails. Confirm PIV App PIN retry counter is decremented by one.	[SP800-73] Part 1, §3.2.6, §5.1	Sev-2
Security	Required	5.17.4	Discovery object is present and set for PIV App PIN only. Confirm E-PACS is using the Application PIN.	Use Card 26 and enter PIV App PIN. Access is granted. Confirm PIV App PIN retry counter is reset to 5.	[SP800-73] Part 1, §3.2.6, §5.1	Sev-2

Security	Required	5.17.5	Discovery object is present. PIV App and Global PINs are available. PIV App PIN is primary. Confirm E-PACS is using the Application PIN.	Use Card 27 and enter invalid PIV App PIN (e.g., 999999). Registration fails. Confirm PIV App PIN retry counter is decremented by one (from 5 to 4). Confirm Global PIN retry counter remains at 5.	[SP800-73] Part 1, §3.2.6, §5.1	Sev-2
Security	Optional	5.17.6	Discovery object is present. PIV App and Global PINs are available. PIV App PIN is primary. Confirm E-PACS is using the Global PIN.	Use Card 27 and enter invalid Global PIN (e.g., 999999). Registration fails. Confirm PIV App PIN retry counter remains at 4. Confirm Global PIN retry counter is decremented by one (from 5 to 4).	[SP800-73] Part 1, §3.2.6, §5.1	Sev-2
Security	Required	5.17.7	Discovery object is present. PIV App and Global PINs are available. PIV App PIN is primary. Confirm E-PACS is using the Application PIN.	Use Card 27 and enter PIV App PIN. Access is granted. Confirm PIV App PIN retry counter reset to 5. Confirm Global PIN retry counter remains at 4.	[SP800-73] Part 1, §3.2.6, §5.1	Sev-2

Security	Optional	5.17.8	Discovery object is present. PIV App and Global PINs are available. PIV App PIN is primary. Confirm E-PACS is using the Global PIN.	Use Card 27 and enter Global PIN. Access is granted. Confirm PIV App PIN retry counter remains at 5. Confirm Global PIN retry counter reset to 5.	[SP800-73] Part 1, §3.2.6, §5.1	Sev-2
Security	Required	5.17.9	Discovery object is present. PIV App and Global PINs are available. Global PIN is primary. Confirm E-PACS is using the Application PIN.	Use Card 28 and enter invalid PIV App PIN (e.g., 999999). Registration fails. Confirm PIV App PIN retry counter is decremented by one (from 5 to 4). Confirm Global PIN retry counter remains at 5.	[SP800-73] Part 1, §3.2.6, §5.1	Sev-2
Security	Optional	5.17.10	Discovery object is present. PIV App and Global PINs are available. Global PIN is primary. Confirm E-PACS is using the Global PIN.	Use Card 28 and enter invalid Global PIN (e.g., 999999). Registration fails. Confirm PIV App PIN retry counter remains at 4. Confirm Global PIN retry counter is decremented by one (from 5 to 4).	[SP800-73] Part 1, §3.2.6, §5.1	Sev-2

Security	Required	5.17.11	Discovery object is present. PIV App and Global PINs are available. Global PIN is primary. Confirm E-PACS is using the Application PIN.	Use Card 28 and enter PIV App PIN. Access is granted. Confirm PIV App PIN retry counter reset to 5. Confirm Global PIN retry counter is reset to 5.	[SP800-73] Part 1, §3.2.6, §5.1	Sev-2
Security	Optional	5.17.12	Discovery object is present. PIV App and Global PINs are available. Global PIN is primary. Confirm E-PACS is using the Global PIN.	Use Card 28 and enter Global PIN. Access is granted. Confirm PIV App PIN retry counter reset to 5. Confirm Global PIN retry counter is reset to 5.	[SP800-73] Part 1, §3.2.6, §5.1	Sev-2
Security	Required	5.17.13	Discovery object is present and tag 0x5F2F is not populated. Confirm E-PACS is using Application PIN.	Use Card 29 and enter invalid PIN (e.g., 999999). Registration fails. Confirm PIV App PIN retry counter is decremented by one.	[SP800-73] Part 1, §3.2.6, §5.1	Sev-2
Security	Required	5.17.14	Discovery object is present and tag 0x5F2F is not populated. Confirm E-PACS is using the Application PIN.	Use Card 29 and enter PIV App PIN. Access is granted. Confirm PIV App PIN retry counter is reset to 5.	[SP800-73] Part 1, §3.2.6, §5.1	Sev-2

		6	Dual Chip Card, time of access	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.** Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	[FIPS 201]	
		6.2	**Signature Verification (Contactless chip on a 2 chip card)**	**These tests are run using a contactless reader. PKI-CAK mode is used for all tests.**		
Security	Required	6.2.1	Verify product’s ability to validate signatures in the certificates found in the certification path for a PIV credential.	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.** Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PIA-2 thru PIA-7	Sev-1
Security	Required	6.2.2	Verify product’s ability to validate signatures in the certificates found in the certification path for a PIV-I credential.	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.** Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PIA-2 thru PIA-7	Sev-1

Security	Required	6.2.3	Verify product’s ability to recognize invalid signature on an intermediate CA in the certification path.	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.** Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PAI-3.2, PIA-3.4, PIA-4, PIA-5	Sev-1
Security	Required	6.2.4	Verify product’s ability to recognize invalid signature on the End Entity certificate.	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.** Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PAI-3.2, PIA-3.4, PIA-4	Sev-1
Security	Required	6.2.5	Verify product’s ability to recognize certificate/private key mismatch.	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.** Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PAI-3.2, PIA-3.4, PIA-4	Sev-1
		7	**PACS Design Use Cases**			

		7.1	**Continuity of Operations Testing**			
Usability	Optional	7.1.1	The network connection is dropped to individual components within the solution individually, in sequence. Degraded mode shall honor requirements for authentication factors and authorizations for a valid credential.	For each component within a solution, disconnect the network to the component. Using Test Card 1: Golden, document success/failure.	PCP-1	Sev-3
Usability	Optional	7.1.2	Individual component services within the solution are stopped individually, in sequence. Degraded mode shall honor requirements for authentication factors and authorizations for a valid credential.	For each service within a solution, manually stop the service on the server(s). Test Card 1: PIV Golden, document success/failure.	PCP-1	Sev-3
Usability	Optional	7.1.3	Power is removed and immediately restored to individual components within the solution, in sequence. Solution shall recover and honor requirements for authentication factors and authorizations for a valid credential.	For each component within the solution, abruptly remove all power sources from the power supply. Restore power. Attempt access with Test Card 1: PIV Golden, document success/failure.	PCP-1	Sev-3
Usability	Optional	7.1.4	The network connection is dropped to individual components within the solution individually, in sequence. Degraded mode shall honor requirements for authentication factors and authorizations for an invalid credential.	Using Test Card 1: Golden, document success/failure.	PCP-1	Sev-3

Usability	Optional	7.1.5	Individual component services within the solution are stopped individually, in sequence. Degraded mode shall honor requirements for authentication factors and authorizations for an invalid credential.	Using Test Card 1: Golden, document success/failure.	PCP-1	Sev-3
Usability	Optional	7.1.6	Power is removed and immediately restored to individual components within the solution, in sequence. Solution shall recover and honor requirements for authentication factors and authorizations for an invalid credential.	Using Test Card 1: Golden, document success/failure.	PCP-1	Sev-3
		7.2	**Security Boundaries**			
Security	Required	7.2.1	...all security relevant processing shall be performed inside the secure perimeter. No security relevant decisions shall be made by system components that do not belong to the cardholder's credential when they are on the attack side of the door.	Confirm all PACS components (except for the reader and the bearer's credential) are capable of being located on the secure side of perimeter. Confirm with protocol sniffing between secure/attack side.	PPE-1	Sev-1

Security	Optional	7.2.2	...compensating controls applied such as tamper switches and FIPS 140-2 certified cryptographic processing within the reader itself.	Specific waivers to 7.2.1 shall be granted on a per implementation basis of compensating controls. Document all supplemental security devices and check against APLs, FIPS 140-2. Confirm controls are operational through physical inspection, design documentation. Confirm with protocol sniffing between secure/attack side.	PPE-1	Sev-1
		7.3	**Registering Physical Access Privileges**			
Usability	Optional	7.3.1	Shall be able to define populations (validities) such as "guest, visitor, and regular access".	Confirm physical inspection and design documentation.	PPL-4	Sev-3
Usability	Optional	7.3.2	Shall be able to define: Access points for each population.	Verify by system design review	PPL-5, PAC-1	Sev-3
Usability	Optional	7.3.3	Shall be able to define: Temporal access rules for each population.	Verify by system design review.	PPL-5, PAC-1	Sev-3
Usability	Optional	7.3.4	Shall be able to define: Authentication mode required to support 7.3.2 and 7.3.3.	Verify by system design review.	PPL-5, PAC-1	Sev-3
		7.4	**PKI Configuration**			

Security	Optional	7.4.1	The solution shall provide the means to select which X.509 constraints are evaluated such as policy constraints, name constraints and key usage. This configuration will reflect the customer's PKI relying party policy.	Verify configurability of X.509 constraints and policies.	PIA-5	Sev-1
Security	Required	7.4.2	The solution shall provide the means to select and manage Trust Anchors. This configuration will reflect the customer's PKI relying party policy.	Verify configurability of trust anchors.	PSC-2	Sev-1
Security	Optional	7.4.3	The solution may provide configuration options to ignore PKI faults in certificates (end-entity up to trust anchor). This configuration will reflect the customer's PKI relying party policy.	Perform design review of vendor's PKI configuration options. If options are presented to ignore PKI faults, testing shall proceed to 7.4.4.		Sev-1
Security	Required	7.4.4	For every event where a PKI fault is identified, the solution shall check configuration options to ignore the identified fault. If configuration allows the solution to ignore the fault, the solution shall ignore the fault and produce a warning in the audit log and store the certificate in a certificate store of failed certificates. The audit log shall indicate what failed and provide sufficient information to link the log entry to the stored certificate.	Configure system to ignore PKI faults one by one, per capability of solution. Re-run appropriate ICAM card and PKI tests for both time of registration and time of access with the appropriate fault. Inspect logs and the linked certificate store. Confirm failure is properly identified and certificate matches log entry.		Sev-2

Security	Required	7.4.5	If PKI faults are allowed, the solution shall provide a means to generate a report and consolidate failed certificates for transmission to appropriate parties by email. Running the report and sending the email shall be per the customer's PKI relying party policy.	Confirm ability to generate report and certificates to be sent by email.		Sev-2
Security	Required	7.4.6	The system shall check that the issuing certificate authority has not placed the certificate on its certificate revocation list (CRL) within the previous 6 hours.	Confirm solution's ability to set CRLs and OCSP response caching to 6 hours or less.		Sev-1
Security	Required	7.4.7	The system shall process revocation progression from OCSP to HTTP CRL. If the system leverages SCVP in lieu of OCSP or HTTP CRL, and SCVP is unavailable, it should support the progression from OCSP to HTTP CRL.	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.** Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.		Sev-2
		7.5	**Credential Number Specifications**			

Security	Required	7.5.1	The solution shall support FICAM conformant 128-bit FASC-N credential numbers as specified in *Table 3* for Time of Registration, Time of Access, and Automated Provisioning.	Configure system for 128-bit FASC-N. Review transactional test logs for registration and access. Confirm all operational usage is 128-bit and not parsed into separate fields. If the system parses the numbers into separate fields, the details shall be provided to the GSA ICAM Lab for testing purposes.	PAU-2, PAU-3; Table 6-1 row 3	Sev-1
Security	Required	7.5.2	The solution shall support FICAM conformant 128-bit UUID credential numbers as specified in *Table 3* for Time of Registration, Time of Access, and Automated Provisioning.	Configure system for 128-bit UUID. Review transactional test logs for registration and access. Confirm all operational usage is 128-bit and not parsed into separate fields. If the system parses the numbers into separate fields, the details shall be provided to the GSA ICAM Lab for testing purposes.	PAU-2, PAU-3; Table 6-1 row 3	Sev-1
		7.6	**Validation at Time of Access**			
Usability	Optional	7.6.2	Shall support contactless Card Authentication Key (PKI-CAK) for Dual Interface Chip card.	Use Authentication Test logs to verify that all good cards were allowed access at the door reader.	PIA-2, PIA-3.x, PIA-4, PIA-5, PIA-6, PIA-7, §10.1.1	Sev-1

Usability	Optional	7.6.3	Shall support BIO.	Use Authentication Test logs to verify that all good cards with valid BIO available were allowed access at the door reader.	PIA-2, PIA-3.x, PIA-4, PIA-5, PIA-6, PIA-7	Sev-1
Usability	Optional	7.6.4	Shall support PIV Authentication Key + PIN (PKI-AUTH).	Use Authentication Test logs to verify that all good cards were allowed access at the door reader.	PIA-2, PIA-3.x, PIA-4, PIA-5, PIA-6, PIA-7, §10.1.2	Sev-1
Usability	Optional	7.6.5	Shall support PIV Authentication Key + PIN + BIO (PKI-AUTH+BIO).	Use Authentication Test logs to verify that all good cards with valid PKI-AUTH and BIO available were allowed access at the door reader.	PIA-2, PIA-3.x, PIA-4, PIA-5, PIA-6, PIA-7, §10.1.5	Sev-1
Usability	Optional	7.6.6	Shall support Card Authentication Key + PIN + BIO (PKI-CAK+BIO).	Use Authentication Test logs to verify that all good cards with valid PKI-CAK and BIO available were allowed access at the door reader.	PIA-2, PIA-3.x, PIA-4, PIA-5, PIA-6, PIA-7, §10.1.4	Sev-1

Usability	Optional	7.6.7	Shall support PKI-CAK + BIO to PACS.	Use Authentication Test logs to verify that all good cards with valid BIO were allowed access at the door reader. Confirm protection of authenticator in the PACS.	PIA-2, PIA-3.x, PIA-6, PIA-3.4 Detailed Guidance Case 3	Sev-1
Usability	Optional	7.6.8	Shall support PKI-AUTH + BIO to PACS.	Use Authentication Test logs to verify that all good cards with valid BIO were allowed access at the door reader. Confirm protection of authenticator in the PACS.	PIA-2, PIA-3.x, PIA-6, PIA-3.4 Detailed Guidance Case 3	Sev-1
Usability	Optional	7.6.9	Shall support contact Card Authentication Key (PKI-CAK) for Dual Interface Chip card.	Use Authentication Test logs to verify that all good cards were allowed access at the door reader.	PIA-2, PIA-3.x, PIA-4, PIA-5, PIA-6, PIA-7	Sev-1
Usability	Optional	7.6.10	Shall support contactless Card Authentication Key (PKI-CAK) for Dual Chip card.	**Will not be tested until new ICAM Test Cards and ICAM Test PKI are available.** Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PIA-2, PIA-3.x, PIA-4, PIA-5, PIA-6, PIA-7	Sev-1

Security	Required	7.6.11	E-PACS portal solutions shall not support legacy technologies when configured for approved FICAM modes.	Verify solution turns off legacy modes when an approved FICAM mode is enabled. With reader set to PKI-AUTH, attempt to use 125KHz, DESFire, iClass, Indala and related legacy technologies. All access attempts with legacy shall be denied.	PIA-2, PIA-3.x, PIA-4, PIA-5, PIA-6, PIA-7	Sev-1
Usability	Optional	7.6.12	Shall support PKI-CAK + PIN to PACS.	Use Authentication Test logs to verify that all good cards with valid PIN were allowed access at the door reader. Confirm protection of authenticator in the PACS.	PIA-2, PIA-3.x, PIA-6, PIA-3.4 Detailed Guidance Case 3, PIA-10, §10.1.3	Sev-1
Security	Required	7.6.13	E-PACS portal solutions shall not support legacy PIV authentication modes when in approved FICAM configuration.	**This requirement becomes effective June 2, 2015.** Verify solution turns off legacy PIV authentication modes described in §10.2 when in approved FICAM configuration. All access attempts with legacy PIV authentication modes shall be denied.	§10.1, §10.1.1, §10.1.2, §10.1.3, §10.1.4, §10.1.5, §10.2	Sev-1
		7.7	**Portal Hardware**			

Security	Required	7.7.1	Product shall support Reader to PACS communications using bi-directional technology. This includes a minimum of one of RS-485, Ethernet, and secure wireless.	Verify by system design review. Confirmed using protocol sniffing, review of logs produced during authentication testing.	PCM-2, PCM-3	Sev-1
Usability	Optional	7.7.2	For multi-factor readers, applicant's system must allow an administrator to modify an individual reader's authentication mode (authentication factors) from the server or a client/workstation to the server.	Verify by system design review. Confirm by setting multi-factor reader authentication modes and using Test card 1: PIV Golden for access according to mode.	PCM-3	Sev-3
Usability	Optional	7.7.3	For multi-factor readers, applicant's system must allow an administrator to modify a group of readers' authentication mode (authentication factors) from the server or a client/workstation to the server.	Verify by system design review. Confirm by setting multi-factor reader authentication modes and using Test card 1: PIV Golden for access according to mode.	PCM-3	Sev-3
Usability	Optional	7.7.4	For multi-factor readers, the site administrator shall not be required to approach and touch each reader to change its authentication mode (authentication factors).	Verify by system design review. Confirm by setting multi-factor reader authentication modes and using Test card 1: PIV Golden for access according to mode.	PCM-3	Sev-3
Usability	Optional	7.7.5	For multi-factor readers, the system shall support dynamic assignment of an individual reader's authentication mode (authentication factors) on a time based schedule.	Verify by system design review. Confirm by setting schedule for multi-factor reader authentication modes and using Test card 1: PIV Golden for access according to mode.	PCM-3	Sev-3

Usability	Optional	7.7.6	For multi-factor readers, the system shall support dynamic assignment of a group of readers' authentication mode (authentication factors) on a time based schedule.	Verify by system design review. Confirm by setting schedule for multi-factor reader authentication modes and using Test card 1: PIV Golden for access according to mode.	PCM-3	Sev-3
Usability	Optional	7.7.7	For multi-factor readers, the system shall support dynamic assignment of an individual reader's authentication mode (authentication factors) based on Threat Condition, Force Protection Condition, Maritime Security Level, or other similar structured emergency response protocol.	Verify by system design review. Confirm by setting emergency response protocol level for multi-factor reader authentication modes and using Test card 1: PIV Golden for access according to mode.	PCM-3	Sev-3
Usability	Optional	7.7.8	For multi-factor readers, the system shall support dynamic assignment of a group of readers' authentication mode (authentication factors) based on Threat Condition, Force Protection Condition, Maritime Security Level, or other similar structured emergency response protocol.	Verify by system design review. Confirm by setting emergency response protocol level for multi-factor reader authentication modes and using Test card 1: PIV Golden for access according to mode.	PCM-3	Sev-3
Usability	Required	7.7.9	Contact readers shall support ISO/IEC 7816.	The contact interface of the reader shall be tested for ISO/IEC 7816 conformance. It is recommended the vendor test in accordance with ISO/IEC 10373-3:2010 Sections 4, 7, and 8. Vendor shall provide a test data report documenting conformance for review and approval.	[FIPS 201]	Sev-2

Usability	Required	7.7.10	Contactless readers shall support ISO/IEC 14443 Type A.	The contactless interface of the reader shall be tested for ISO/IEC 14443 Type A conformance. It is recommended the vendor test in accordance with ISO/IEC 10373-6:2011 Sections 4, 5, 6.1, 7.1 and 8.1, and ISO/IEC 10373-6:2011/Amd.4:2012. Vendor shall provide a test data report documenting conformance for review and approval.	[FIPS 201]	Sev-2
Security	Required	7.7.11	ISO/IEC 14443 Type A contactless readers shall not activate and operate with a PIV card beyond 10cm.	Card 1 is presented at 11cm to the reader. All contactless PIV authentication modes shall fail.	[FIPS 201]	Sev-3
Usability	Required	7.7.12	ISO/IEC 14443 Type A contactless readers shall provide sufficient field strength to activate and operate with a PIV card at or below 3.5cm.	Card 1 is presented at 3.5cm to the reader. All contactless PIV authentication modes shall succeed.	[FIPS 201]	Sev-3
Security	Optional	7.7.13	The System shall protect the communications between readers and the PACS using a cryptographically secure protocol.	FICAM profile to be developed in next spiral of FIPS 201 Evaluation Program (may include use of OSDP).	PSC-1	Sev-3
Usability	Optional	7.7.14	For multi-factor readers, if a time delay of longer than 120 seconds is required for a reader to change modes, this too shall be considered non-compliant.	Verify by system design review.	PCM-3	Sev-3
		7.8	**Auditing and Logging**			

Security	Required	7.8.1	Granularity of auditing records shall be to the card and individual transaction. These shall be easily verifiable through a reporting tool or any other log and audit viewing capability.	Verify by review of logs and reports.	PAU-1, PAU-2, PAU-7	Sev-2
Security	Required	7.8.2	The product shall provide auditing/logging of all PKI processing to include: • Pass/fail from a Challenge/Response • PDVAL • Disabling credential based on PDVAL, expiration, or revocation status	Verify by review of logs and reports; confirmed by protocol sniffing.	PAU-3, PAU-4, PAU-7	Sev-1
Security	Required	7.8.3	The product shall provide auditing/logging of credential number processing and transmission.	Verify by review of logs and reports.	PAU-4, PAU-5, PAU-7	Sev-2
Security	Required	7.8.4	The product shall provide auditing/logging of all software driven configuration changes.	Verify by review of logs and reports.	PAU-6, PAU-7	Sev-2
Security	Required	7.8.5	The product shall provide auditing/logging of periodic certificate PDVAL and status checking.	Verify by review of logs and reports.	PAU-4, PAU-5, PAU-7	Sev-2
Security	Required	7.8.6	The product shall provide auditing/logging of Card activity (e.g., 3 days of card activity).	Verify by review of logs and reports.	PAU-3, PAU-7	Sev-2
Security	Required	7.8.7	The product shall provide auditing/logging of last known location of a card in system.	Verify by review of logs and reports.	PAU-3, PAU-7	Sev-2

Security	Required	7.8.8	The product shall provide auditing/logging of PKI policies for name constraints, path constraints, and validity checks.	Verify by review of logs and reports.	PAU-4, PAU-5, PAU-7	Sev-2
Security	Required	7.8.9	The product shall provide auditing/logging of individual and group reporting of alarms (e.g., door force, door prop).	Verify by review of logs and reports.	PAU-3, PAU-7	Sev-2
Security	Required	7.8.10	The product shall provide auditing/logging of what date individuals were provisioned or de-provisioned and by whom.	Verify by review of logs and reports.	PAU-4, PAU-7	Sev-2
Security	Required	7.8.11	The product shall provide auditing/logging of all readers and their modes.	Verify by review of logs and reports.	PAU-5, PAU-6, PAU-7	Sev-2
Security	Required	7.8.12	The product shall provide auditing/logging of configuration download status to system components.	Verify by review of logs and reports.	PAU-5, PAU-6, PAU-7	Sev-2
		7.9	**Security Certification and Accreditation**			
Usability	Required	7.9.1	As required by UL 294, relevant components within the solution shall have a UL 294 listing.	Verify UL listing. Must be listed before final testing and certification by FIPS 201 Evaluation Program.	PCA-2	Sev-1
Usability	Required	7.9.2	As required by UL 1076, relevant components within the solution shall have a UL 1076 listing.	Verify UL listing. Must be listed before final testing and certification by FIPS 201 Evaluation Program.	PCA-2 derived	Sev-3

Usability	Required	7.9.3	As required by UL 1981, relevant components within the solution shall have a UL 1981 listing.	Verify UL listing. Must be listed before final testing and certification by FIPS 201 Evaluation Program.	PCA-2 derived	Sev-3
Usability	Required	7.9.4	When adding a component to an existing system under a given topology, each existing component in the existing system under that topology shall have GSA FIPS-201 Evaluation Program APL status.	Verify APL listing. Must be listed before final testing and certification by FIPS 201 Evaluation Program.	PCA-3	Sev-1
Security	Required	7.9.5	Each component leveraging cryptography in the system shall have FIPS 140-2 certification.	Verify NIST CMVP listing. Must be applied for and in process for certification before any testing can be done. Must be listed before final testing and certification by FIPS 201 Evaluation Program.	PCA-4	Sev-1
Security	Required	7.9.6	All components of the solution shall be certified against [BAA] requirements.	Review Attestation from application.		Sev-1
Security	Required	7.9.7	All components of the solution shall be certified against [TAA] requirements.	Review Attestation from application.		Sev-1
		7.10	**Biometric in PACS**			
Security	Optional	7.10.1	Shall follow PIA-3.4 Detailed Guidance Case 3 for biometric identifiers leveraged in BIO to PACS.	Verify by system design and inspection of database.	PIA-3.4	Sev-1
		7.11	**Operational Controls**			

Security	Required	7.11.1	The system shall have the ability to enforce administrative privilege for configuration management operations.	Verify by use of the system.	PCM-1	Sev-2
Security	Required	7.11.2	Shall authenticate administrators using a process of equivalent or greater assurance than the authentication modes supported by the system. This may be done using E-Authentication LOA-4 credentials.	Verify by use of the system.	PCM-1	Sev-2
Usability	Optional	7.11.3	The system shall have the ability to manage the system through software controlled configuration management methods. Initial configuration of hardware settings (e.g., DIP switches) is allowed at installation only and not for management of the hardware tree.	Verify by use of the system.	PCM-2	Sev-3
Usability	Optional	7.11.4	Each physical component shall be separately defined and addressable within the server user interface.	Verify by setting up of system.	PCM-2	Sev-3
Usability	Optional	7.11.5	The system shall support configuration downloads to relevant components.	Verify by setting up of system.	PCM-2	Sev-3
		7.12	**Accessibility**			

Usability	Required	7.12.1	All components in the end-to-end solution shall support [Sect508] of the Rehabilitation Act[2].	Review Attestation from application.	Section 508 of the Rehabilitation Act	Sev-2
		8.	**Handheld Requirements**			
		8.1.	**Communications**			
Security	Required	8.1.1.	Ensure a secure connection using an encrypted wireless session using a NIST certified encryption method.	Verify within the handheld settings that there is an option to encrypt communications using NIST approved methods.		Sev-1
Security	Required	8.1.2.	Must have built-in support for Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2).	Verify within the handheld settings that the interface supports a minimum of WPA. WPA-2 is preferred.		Sev-1
Usability	Optional	8.1.3.	The system has the ability to communicate using 802.11 a, b, c, g, n.	Verify within the handheld settings that the wireless interface supports one of the listed protocols.		Sev-2
Usability	Required	8.1.4.	The Handheld must be able to support both 3G and 4G communications for cellular communications.	Verify within the handheld settings that the option for 3G or 4G communications exists.		Sev-2

[2] The FIPS 201 Evaluation Program has no jurisdiction with respect to installation of the solution in order to meet [Sect508] requirements. This attestation requires the user interface (including visual, audio, and touch) to be [Sect508] compliant for all components within the end-to-end solution.

Usability	Optional	8.1.5.	Handheld must have the ability to demonstrate the option to select a primary communication source and a secondary communication source.	Verify the reader interface allows the devices to be configured for a primary and secondary method of communications.		Sev-3
Usability	Optional	8.1.6.	Handheld must be able to failover from primary to secondary mode to maintain an online state with PACS and Validations system.	Verify that if wireless communications is lost, the reader attempts to connect to secondary mode of communications.		Sev-3
Usability	Required	8.1.7.	Reader provides a visual indication that the handheld is in an online or offline state.	Verify the reader provides an indication that the reader is in an offline state.		Sev-1
		8.2.	**Operational Requirements**			
Usability	Required	8.2.1.	The handheld must be capable of supporting contactless, contact, or both modes of authentication. Interfaces can be fully integrated or modular.	Verify the handheld has at least one mode of authentication.		Sev-1
Usability	Optional	8.2.2.	Contactless modes must support a minimum of: • CAK+CHUID	Test Contactless interface and confirm access grant.		Sev-1
Usability	Optional	8.2.3.	Contact modes must support a minimum of: • CAK+CHUID • PIV+PIN • PIV+PIN+BIO	Test contact interface in all supported modes and confirm access grant.		Sev-1

		8.3.	**Docking Station**	**If a docking station exists**		
Usability	Required	8.3.1.	The handheld docking station must utilize a hardwired Ethernet port or wireless communications with the Validation System, PACS, or other trusted source.	Verify the docking station provides at least one method of network communication.		Sev-1
Security	Required	8.3.2.	The handheld docking station provides a mechanism to securely update the handheld while cradled in the device, via hardwired Ethernet or Wireless communications. Updates can be from online validation system, PACS or other trusted source.	Secure communication enforced by mutual authentication TLS with PKI.		Sev-1
Security	Required	8.3.3.	Handheld must automatically logout operator when placed in docking station.	Verify if the operator has not logged out of the Handheld, ensure the handheld automatically logs the operator out.		Sev-1
		8.4.	**FINGERPRINT Verification**	**If BIO Authentication Method is Supported, tests in this section are Required.**		
Security	Optional	8.4.1.	• See Section 2 – Validation at time of Registration • See Section 5 – Validation at time of Access			Sev-1
		8.5.	**Import Function**			

Usability	Required	8.5.1.	Reader must cache CRL information locally on the handheld This CRL data must include the Certificate PATH information and be supplied by an online Validation System or other trusted source.	Verify the reader's ability to store locally cached CRL.		Sev-1
Usability	Required	8.5.2.	Cached information must be protected either by a FIPS140-2 level -1software or Level-2 HSM.	Verify the handheld has mitigated the risk to keying material using FIPS140 approved encryption methods.		Sev-1
Security	Required	8.5.3.	The reader must cache authentication and authorization information for all cardholders with access to the Handheld assigned area. This information can be transferred from either an online validations system or other trusted source.	Verify the local database is storing the authentication and authorization information for registered and provisioned card holders in the local handheld database.		Sev-1
Security	Required	8.5.4.	The Handheld device must have the ability to provide a visual indication when locally cached information is over 6 hours old.	Verify the operator is notified when locally cached information is over 6 hours old.		Sev-1
		8.6.	**Operational**			
Security	Required	8.6.1.	System must automatically log the operator out of the handheld after a user defined time of non-use.	Verify the handhelds ability to set a time out period. This time out period should automatically log the operator out of the handheld one the threshold has been reached.		Sev-1

Security	Required	**8.7.**	**Online Validation Requirements**			
Security	Required	8.7.1.	When the Handheld is online communicating with the Validations System, functional requirements defined within the Validation System category apply.	Must comply with: • Section 5, Authentication at Time of Access, in this document		Sev-1
Security	Required	**8.8.**	**Online PACS Requirements**			
Security	Required	8.8.1.	When the Handheld is online communicating with the PACS. The PACS functional requirements defined in the PACS Infrastructure category apply.	Must Comply with: • Section 5, Validation at Time of Access, in this document • Section 7, PACS Design use Cases, in this document		Sev-1
		8.9.	**Offline Validation Requirements**			
Security	Required	8.9.1.	Handheld must use locally cached authentication and authorization data to authenticate and authorize the operator.	While reader is in offline mode verify the operator can login and access the application based on assigned privileges.		Sev-1
Security	Required	8.9.2.	Handheld must be able to determine the validity of the cardholder certificates using the locally cached validation data.	While reader is in offline mode and using Golden Card-1 verify the handhelds ability to validate the card against locally stored validation database.		Sev-1

Security	Required	8.9.3.	Handheld must provide the operator with indication that the locally stored data exceeds 6 hour refresh limit.	While reader is offline advance the clock to exceed local cache timestamp by 6hrs. Confirm the operator is provide with an indication that the local cache needs to be refreshed.		Sev-1
Security	Required	8.9.4.	Handheld must cache PKI Validation decisions to be uploaded to the trusted source for archive and reporting.	While the reader is offline run a series of positive and negative test case cards. Return reader to online state and verify tracks actions are imported to the trusted source.		Sev-1
		8.10.	**Offline PACS Requirements**			
Security	Required	8.10.1.	The handheld must provide an indication to the operator that the reader is in offline mode.	Disconnect handheld from network and verify operator is provided an offline indication.		Sev-1
Security	Required	8.10.2.	The handheld must be able to use locally cached PACS data to verify cardholders access privileges. For example: • Schedule • Shift • Access to areas The operator must be provided a visual indication of access granted or denied.	While offline use golden card to verify access is granted and visual indication is provided to operator.		Sev-1

Security	Required	8.10.3.	While in offline mode the handheld must log all access decisions made at the handheld.	Verify the handhelds ability to store access transaction data locally.		Sev-1
Security	Required	8.10.4.	When transitioning from an offline to an online state the handheld must transfer all locally stored access transaction to the PACS solution or other trusted source.	Verify that transactions logged in Test Case 12.5.3 are transferred to the PACS solution or trusted source.		Sev-1

Appendix 2 Deprecated Test Cases

The table below lists test cases that have been deprecated from the FRTC. These tests have become obsolete. Some have been replaced with another test case. Test cases for a particular security risk may have been mitigated by another technology or standard.

Security/ Usability	Required or Optional	Test	Requirement	Test Case: Pass/Fail criteria	Requirement Source	Deprecated Date
Security	Required	2.4.2	Verify product's ability to recognize when the *basicConstraints* extension is present and critical in the intermediate CA certificate but the CA component is false.	Deprecated. Criticality is not the driver. Honoring the *basicConstrants* is the critical issue. Card 1: (Golden PIV Card) w/PKI Path 6 fails to register successfully.	PIA-3.2, PIA-5	6/2/2014
Security	Required	2.4.3	Verify product's ability to recognize when the *basicConstraints* extension is present and not critical in the intermediate CA certificate but the CA component is false.	Deprecated. Criticality is not the driver. Honoring the *basicConstrants* is the critical issue. Card 1: (Golden PIV Card) w/PKI Path 7 fails to register successfully.	PIA-3.2, PIA-5	6/2/2014

Security/ Usability	Required or Optional	Test	Requirement	Test Case: Pass/Fail criteria	Requirement Source	Deprecated Date
Security	Required	2.4.6	Verify product's ability to detect a mismatched AKID with the authority (issuer) public key in the certificate.	Deprecated. This test case was determined to be unnecessary. A mismatched AKID usually indicates an Issuer interoperability problem rather than a path building/validation problem. Card 1: (Golden PIV Card) w/PKI Path 33 fails to register successfully.	PIA-3.2, PIA-5	6/2/2014
Security	Required	2.5.2	Verify product's ability to recognize when the intermediate certificate includes a non-critical *keyUsage* extension.	Deprecated. Criticality is not the driver. Honoring the *keyUsage* is the critical issue. Card 1: (Golden PIV Card) w/PKI Path 10 fails to register successfully.	PIA-3.2, PIA-5	6/2/2014

Security/ Usability	Required or Optional	Test	Requirement	Test Case: Pass/Fail criteria	Requirement Source	Deprecated Date
Security	Required	2.6.6	With no policy set, verify product's ability to process *requiredExplicitPolicy*.	Deprecated. This test case was designed around the certificate extension for Policy Constraints and the purpose was determined to be redundant with other requirements that systems understand how to require and filter for explicit certificate policies. Card 1: (Golden PIV Card) w/PKI Path 22 fails to register successfully.	PIA-3.2, PIA-5	6/2/2014
Security	Required	2.6.7	With required policy set to 2.16.840.1.101.3.2.1.48.11 (test id-fpki-common-authentication), verify product's ability to process a path with an invalid setting for *requiredExplicitPolicy*.	Deprecated. This test case was designed around the certificate extension for Policy Constraints and the purpose was determined to be redundant with other requirements that systems understand how to require and filter for explicit certificate policies. Card 1: (Golden PIV Card) w/PKI Path 23 fails to register successfully.	PIA-3.2, PIA-5	6/2/2014

Security/ Usability	Required or Optional	Test	Requirement	Test Case: Pass/Fail criteria	Requirement Source	Deprecated Date
Security	Required	2.17.1	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (1024).	Deleted. (valid through 1/1/2014) NIST card#7 registers successfully.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5	6/2/2014
Security	Optional	2.17.4	Verify Product's ability to validate signatures using RSASSA-PSS (1024).	Deprecated. (valid through 1/1/2014)	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5	6/2/2014
Security	Optional	2.17.9	Verify Product’s ability to validate signatures using SHA-1.	Deprecated. NIST card#7 registers successfully.	[SP800-78] Table 3-7; [Common] §6.1.5	6/2/2014
Security	Required	5.4.2	Verify product's ability to recognize when the *basicConstraints* extension is present and critical in the intermediate CA certificate but the CA component is false.	Deprecated. Criticality is not the driver. Honoring the *basicConstrants* is the critical issue. Card 1: (Golden PIV Card) fails access grant w/PKI Path 6.	PIA-3.2, PIA-5	6/2/2014

Security/ Usability	Required or Optional	Test	Requirement	Test Case: Pass/Fail criteria	Requirement Source	Deprecated Date
Security	Required	5.4.3	Verify product's ability to recognize when the *basicConstraints* extension is present and not critical in the intermediate CA certificate but the CA component is false.	Deprecated. Criticality is not the driver. Honoring the *basicConstrants* is the critical issue. Card 1: (Golden PIV Card) fails access grant w/PKI Path 7.	PIA-3.2, PIA-5	6/2/2014
Security	Required	5.4.6	Verify product’s ability to detect a mismatched AKID with the authority (issuer) public key in the certificate.	Deprecated. This test case was determined to be unnecessary. A mismatched AKID usually indicates an Issuer interoperability problem rather than a path building/validation problem. Card 1: (Golden PIV Card) w/PKI Path 33 receives access denied.	PIA-3.2, PIA-5	6/2/2014
Security	Required	5.5.2	Verify product’s ability to recognize when the intermediate certificate includes a non-critical *keyUsage* extension.	Deprecated. Criticality is not the driver. Honoring the *keyUsage* is the critical issue. Card 1: (Golden PIV Card) fails access grant w/PKI Path 10.	PIA-3.2, PIA-5	6/2/2014

Security/ Usability	Required or Optional	Test	Requirement	Test Case: Pass/Fail criteria	Requirement Source	Deprecated Date
Security	Required	5.6.6	With no policy set, verify product's ability to process *requiredExplicitPolicy*.	Deprecated. This test case was designed around the certificate extension for Policy Constraints and the purpose was determined to be redundant with other requirements that systems understand how to require and filter for explicit certificate policies. Card 1: (Golden PIV Card) w/PKI Path 22 receives access denied.	PIA-3.2, PIA-5	6/2/2014
Security	Required	5.6.7	With required policy set to 2.16.840.1.101.3.2.1.48.11 (test id-fpki-common-authentication), verify product's ability to process a path with an invalid setting for *requiredExplicitPolicy*.	Deprecated. This test case was designed around the certificate extension for Policy Constraints and the purpose was determined to be redundant with other requirements that systems understand how to require and filter for explicit certificate policies. Card 1: (Golden PIV Card) w/PKI Path 23 receives access denied.	PIA-3.2, PIA-5	6/2/2014

Security/ Usability	Required or Optional	Test	Requirement	Test Case: Pass/Fail criteria	Requirement Source	Deprecated Date
Security	Required	5.9.9	The system recognizes when an incorrectly formatted CRL is present in the path.	Deprecated. Chasing CDP from the certificate on the card at time of access should never happen. CDP should only be trusted based on registration process. Card 1: (Golden PIV Card) fails access grant w/PKI Path 34.	PIA-3.5, PIA-5, PIA-7	6/2/2014
Security	Required	5.9.10	The system recognizes when an invalid CRL signer is in the path.	Deprecated. Chasing CDP from the certificate on the card at time of access should never happen. CDP should only be trusted based on registration process. Card 1: (Golden PIV Card) fails access grant w/PKI Path 36.	PIA-3.5, PIA-5, PIA-7	6/2/2014
		5.10	**CHUID Verification**	The CHUID Authentication Method is **DEPRECATED**.	[FIPS 201]	6/2/2014

Security	Required	5.16.1	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (1024).	Deprecated.
				(valid through 1/1/2014)
				NIST card#7 is granted access.
					[SP800-78] Table 3-1;
					[SP800-78] Table 3-3;
					[Common] §6.1.5
						6/2/2014

Security/ Usability	Required or Optional	Test	Requirement	Test Case: Pass/Fail criteria	Requirement Source	Deprecated Date
Security	Optional	5.16.4	Verify Product's ability to validate signatures using RSASSA-PSS (1024).	Deprecated. (valid through 1/1/2014)	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5	6/2/2014
Security	Optional	5.16.9	Verify Product's ability to validate signatures using SHA-1.	Deprecated. NIST card#7 is granted access.	[SP800-78] Table 3-7; [Common] §6.1.5	6/2/2014
		6.1	**CHUID Verification (Contactless chip on a 2 chip card)**	The CHUID Authentication Method is **DEPRECATED**.	[FIPS 201]	6/2/2014
Security	Required	7.3.5	No credential shall be individually registered for which there is no valid trust path per the relying party PKI policy.	Deprecated. Duplicative. Derive from the overall results of testing in Section 2.	PIA-9	6/2/2014
Security	Required	7.3.6	No credential shall be individually registered where the binding of the credential to the bearer does not meet relying party security policy.	Deprecated. Duplicative. Derive from the overall results of testing in Section 2.	PIA-9	6/2/2014

Security/ Usability	Required or Optional	Test	Requirement	Test Case: Pass/Fail criteria	Requirement Source	Deprecated Date
Security	Required	7.3.7	No credential shall be individually authorized for access that does not meet relying party security policy.	Deprecated. Duplicative. Derive from the overall results of testing in Section 2.	PIA-9	6/2/2014
Security	Required	7.5.3	Systems that reduce credential numbers defined in *Table 3* to less than 128-bits within any element of the E-PACS solution shall provide compensating controls to avoid credential number collisions. The method shall achieve credential numbers that are greater than or equal to 64-bits. Compensating controls will be deprecated on 10/21/2014.	Perform design review of vendor's compensating controls. Analyze compensating controls to confirm effective credential numbers are greater than or equal to 64-bits.	PAU-2, PAU-3; Table 6-1 row 3 derived	10/21/14
Usability	Optional	7.5.4	For 48-bit binary FASC-N ID, the solution shall be configurable to support FICAM conformant credential numbers as specified in **Error! Reference source not found.** for Time of Registration, Time of Access, and Automated Provisioning. This format will be deprecated on 10/21/2014.	Configure system for 48-bit FASC-N ID. Review transactional test logs for registration and access.	PAU-2, PAU-3; Table 6-1 row 3	10/21/14

Security/ Usability	Required or Optional	Test	Requirement	Test Case: Pass/Fail criteria	Requirement Source	Deprecated Date
Usability	Optional	7.5.5	For 64-bit FASC-N ID + CS + ICI, the solution shall be configurable to support FICAM conformant credential numbers as specified in **Error! Reference source not found.** for Time of Registration, Time of Access, and Automated Provisioning. This format will be deprecated on 10/21/2014.	Configure system for 64-bit FASC-N ID + CS + ICI. Review transactional test logs for registration and access.	PAU-2, PAU-3; Table 6-1 row 3	10/21/14
Usability	Optional	7.5.6	For 200-bit Full FASC-N, the solution shall be configurable to support FICAM conformant credential numbers as specified in **Error! Reference source not found.** for Time of Registration, Time of Access, and Automated Provisioning. This format will be deprecated on 10/21/2014.	Configure system for 200-bit Full FASC-N. Review transactional test logs for registration and access.	PAU-2, PAU-3; Table 6-1 row 3	10/21/14
Security	Required	7.5.7	Systems that use legacy/transitional state FASC-N credential numbers defined in **Error! Reference source not found.** shall provide compensating controls to avoid credential number collisions. The method shall achieve	Perform design review of vendor’s compensating controls. Analyze compensating controls to confirm effective credential numbers are greater than or equal to 64-bits.	PAU-2, PAU-3; Table 6-1 row 3 derived	10/21/14

Security/ Usability	Required or Optional	Test	Requirement	Test Case: Pass/Fail criteria	Requirement Source	Deprecated Date
			credential numbers that are greater than or equal to 64-bits. Compensating controls will be deprecated on 10/21/2014.			
Usability	Optional	7.6.1	Shall support Signed CHUID.	Deprecated.	PIA-2, PIA-3.x, PIA-4, PIA-5, PIA-6, PIA-7	2/24/15

Appendix 3 Deprecated ICAM PKI Paths

ICAM PKI Path Number	Fault description	Operational Group	Reason	Deprecated Date
26	ICAM SHA-1 ECDSA prime256v1	Deprecated	Invalid test. Uses SHA-1 not SHA-256	2/17/15
27	ICAM SHA-1 ECDSA secp384r1	Deprecated	Invalid test. Uses SHA-1 not SHA-256	2/17/15
28	ICAM Invalid ECC Signature p256	Deprecated	Invalid test. Uses SHA-1 not SHA-256	2/17/15
29	ICAM Invalid Policy Mapping p256	Deprecated	Invalid test. Uses SHA-1 not SHA-256	2/17/15
30	ICAM Invalid ECC Signature secp384r1	Deprecated	Invalid test. Uses SHA-1 not SHA-256	2/17/15
31	ICAM Invalid Policy Mapping secp384r1	Deprecated	Invalid test. Uses SHA-1 not SHA-256	2/17/15

Appendix 4 Severity Levels

If [FRTC] functional requirements are revised due to time-sensitive security threats, noted technology vulnerabilities, or other critical issues, or alternatively, specific problems are discovered in a vendor's product (or class of products) after it has been listed on the APL, the affected vendor(s) will be notified that the identified product(s) must be improved as necessary in order to remain on the APL. A remediation grace period will be granted commensurate with the severity level of the problem.

Table 44 specifies the remediation timeframes for each severity level. Products not corrected within the given timeframe will be moved to the RPL.

Table 55 specifies the guidelines for Low, Moderate, and High impacts per core area examined. The Program, in collaboration with applicable stakeholders as needed, determines whether an identified problem has Low, Moderate, or High impact. Impact to security, PACS operations, and PACS availability are examined. Other areas may be examined as necessary. The impact of the identified problem is the high water mark impact of the areas examined.

Table 4 - Severity Remediation Timeframes

Severity Level	Severity Description	Remediation Timeframe
1	The identified problem results in a High impact to any of security, PACS operations, PACS availability, or other area examined.	30 days
2	The identified problem results in a Moderate impact to any of security, PACS operations, PACS availability, or other area examined.	90 days
3	The identified problem results in a Low impact to any of security, PACS operations, PACS availability, or other area examined.	1 year

Table 5 - Impact Guidelines

	High	Moderate	Low
Security	Could lead to incorrect access to exclusion areas (see NIST SP 800-116)	Could lead to incorrect access to limited areas (see NIST SP 800-116)	Could lead to incorrect access to controlled areas (see NIST SP 800-116)
Operations	Unable to manage or use the PACS to the extent that PACS use is severely diminished, inconvenient , or unreliable	Unable to manage or use the PACS to the extent that PACS use is seriously diminished, inconvenient, or unreliable	Unable to manage or use the PACS to the extent that PACS use is slightly diminished or inconvenient
Availability	The PACS is down for significant amounts of time, precluding entry into facilities/areas during that time	The PACS is down frequently for limited amounts of time, precluding entry into facilities/areas during those somewhat frequent times	The PACS is down infrequently for limited amounts of time, precluding entry into facilities/areas during those times